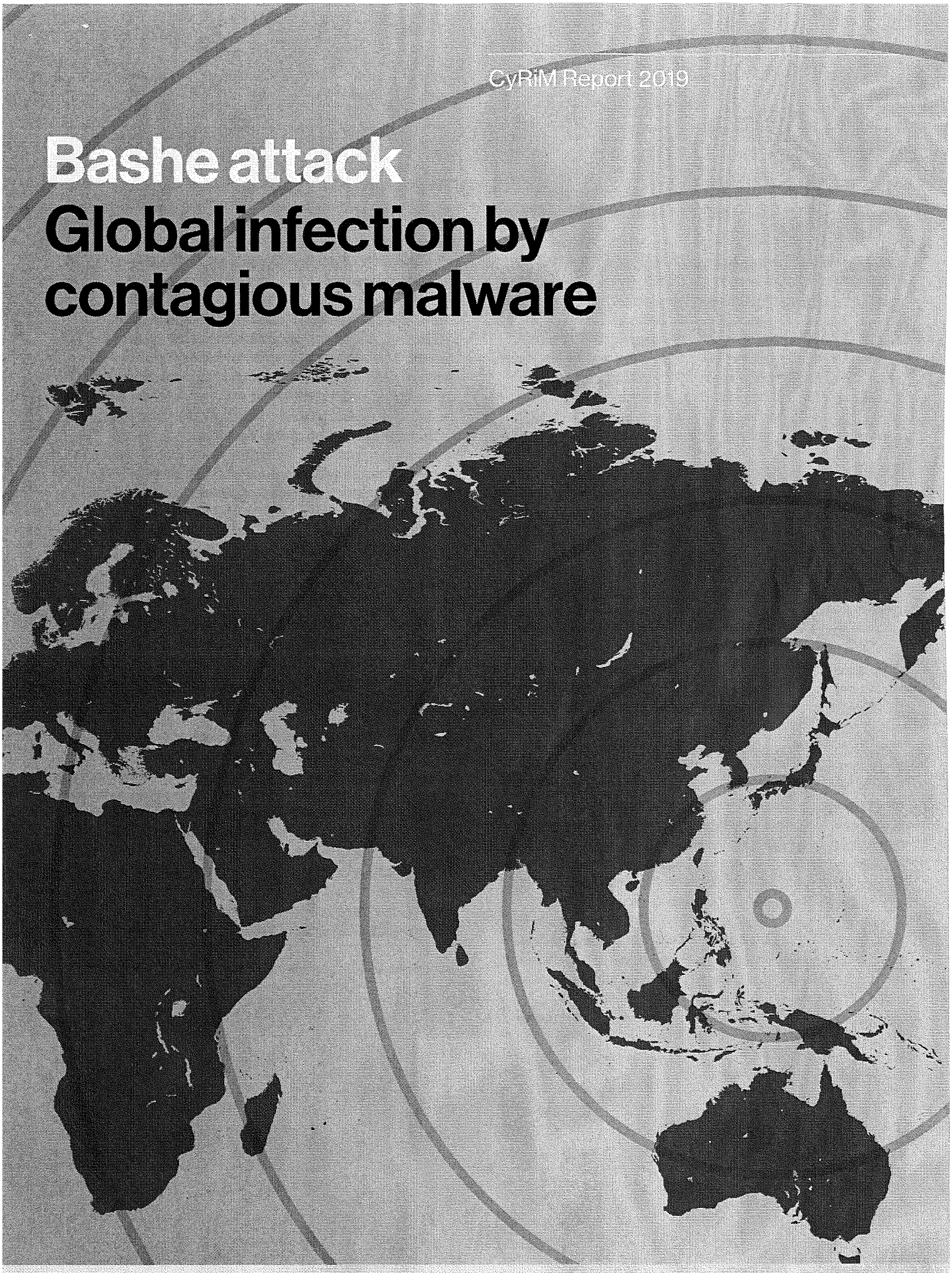
CyRiM Report 2019

Bashe attack
Global infection by contagious malware



NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE
LLOYD'S
AON
MSIG
SCOR The Art & Science of Risk
Transfre
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 to 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 Centre for Innovation and Analytics, 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 of 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 Centre for Innovation and Analytics, 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

Global Infection by Contagious Malware Scenario Research Project Team
- Simon Ruffle, Director of Research and Innovation
- Dr Jennifer Daffron, Research Associate
- Dr Andrew Coburn, Director of Advisory Board
- Jennifer Copic, Research Associate
- Timothy Douglas, Research Assistant
- Eireann Leverett, Senior Risk Researcher
- Olivia Majumdar, Editor
- Kelly Quantrill, Research Assistant
- Andrew Smith, Research Assistant

Cambridge Centre for Risk Studies Research Team
- James Bourdeau, Research Assistant
- Oliver Carpenter, Research Assistant
- Tamara Evan, Research Assistant
- Ken Deng, Research Assistant
- Arjun Mahalingam, Research Assistant
- Professor Danny Ralph, Academic Director
- Kayla Strong, Research Assistant
- Dr Michelle Tuveson, Executive Director

Report Citation:

Cambridge Centre for Risk Studies, Lloyd's of London and Nanyang Technological University, *Bashe attack: Global infection by contagious malware*, 2019

Or

Daffron, J., Ruffle, S., Andrew, C., Copic, J., Quantrill, K., Smith. A., Leverett, E., Cambridge Centre for Risk Studies, *Bashe Attack: Global Infection by Contagious Malware*, 2019

Insurance industry interviews and consultation
- Mark Lynch, AON Centre for Innovation and Analytics
- Alessandro Lezzi, Beazley
- Giles Stockton, Brit
- Nick Barter, Chaucer
- Ian Pollard, Delta Insurance
- Matt Harrison, Hiscox
- David Singh, MS Amlin
- John Brice, MSIG
- Joel Pridmore, Munich Re Syndicate Singapore
- Tim Allen, RenaissanceRe
- Sebastien Heon, SCOR
- Grace Lim, TransRe
- Rhett Hewitt, TransRe

Lloyd's project team
- Dr Trevor Maynard, Innovation
- Angela Kelly, Commercial
- Dr Keith Smith, Innovation
- Pavlos Spyropoulos, Commercial
- Anna Bordon, Innovation
- Ronald Chua, Commercial
- Linda Miller, Marketing and Communications
- Elaine Quek, Marketing and Communications
- Kieran Quigley, Marketing and Communications
- Flemmich Webb, Speech and Studies
- Emma Watkins, Risk Aggregation
- Simon Sherriff, Risk Aggregation

Lloyd's Market Association
- Mel Goddard, Market Liaison & Underwriting Director
- 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 that wish to remain anonymous.

Contents

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 Centre for Innovation and Analytics
- 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

'Bashe attack: Global infection by contagious malware' is the first 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 Centre for Innovation and Analytics, Lloyd's - the specialist insurance and reinsurance market, MSIG, SCOR and TransRe.

Cyber-attacks pose an increasingly severe threat to the global economy. Society's reliance on technology and increased connectivity means it is more vulnerable than ever to malicious software, or malware as it is known.

While several cyber-attacks have spread across the world in a matter of minutes, there has yet to be a coordinated attack that causes catastrophic-level losses. This report models such an attack through a hypothetical scenario in which the devices of hundreds of thousands of companies are infected with ransomware – malware that threatens to destroy or block access to files unless a ransom is paid.

This report explores how a ransomware attack might take place and what the impacts would be on governments, businesses, and the insurance sector.

In the scenario, the malware enters company networks through a malicious email, which, once opened, encrypts all the data on every device connected to the network. The email is forwarded to all contacts automatically to infect the greatest number of devices. Companies of all sizes and in all sectors are forced to pay a ransom to decrypt their data or to replace their infected devices.

Other costs accrue as the scenario unfolds including cyber incident response, damage control and mitigation, business interruption, lost revenue, and reduced productivity. The report analyses the costs of the scenario using three levels of severity with S1 being the least and X1 the most severe.

The scenario shows how exposed society is to such an attack and how much it would disrupt and cost the global economy.

Key findings

Total economic losses

The scenario shows the economic damage to the world economy from a concerted global cyber-attack propagated via malicious email may range from between $85 billion (in the least severe scenario variant, S1) to $193 billion (in the most severe scenario variant, X1).

Economic losses by industry sector

In the S1 scenario, retail suffers the highest total economic loss globally ($15 billion), followed by healthcare ($10 billion) and manufacturing ($9 billion). In X1 retail and healthcare would be the most affected ($25 billion each), followed by manufacturing ($24 billion).

In retail, the malware's encryption of payment systems in traditional retail outlets causes a significant decline in sales revenue while the attack lasts. E-commerce retail revenue is also affected as websites struggle to process web traffic and payment systems fail.

Healthcare is the second-most impacted sector due to the malware's penetration of legacy systems on old healthcare IT equipment that are difficult to clean up and patch. Replacing these systems is costly. This causes significant delays in the recovery process and leads to loss of revenue. Historically. the healthcare sector has been vulnerable to high levels of malware infection due to legacy IT infrastructure systems, which are more vulnerable to malware, and low investment in IT.

The manufacturing sector suffers significant revenue loss because the malware encrypts manufacturing equipment which halts production. The encryption of inventory management systems further disrupts production. The indirect impact on international trade causes delays in the transportation of 'final' goods these companies produce as well as intermediary goods needed for production. This causes further disruption and revenue loss.

Economic losses by region

The negative economic consequences of the scenario are experienced across the globe. The region with the highest total economic loss is the US, followed by Europe, Asia, and the Rest of the World.

	S1	S2	X1
Total economic loss global ($bn)	$85	$159	$193
US	$46	$77	$89
Europe	$30	$61	$76
Asia	$6	$14	$19
Rest of the World	$3	$7	$9

The US economic loss, which ranges from $46-89 billion is driven primarily by the infection of premier-sized companies, particularly within the service sectors such as finance, healthcare and retail. High infection rates in the finance sector cause significant disruption to the US financial markets.

In Europe, the second-most affected region, with $30-76 billion at stake, retail, business and professional services, and manufacturing are the hardest hit sectors. One reason the financial costs are lower than in the US is that the malware infects a much higher number of small and medium-sized enterprises and a lower number of premier-sized companies. This penetration of SMEs in Europe and the relatively high infection rate of small companies (due to poor cyber defences - see Section 3) increases the number of businesses infected but due to the low potential revenue loss per day for small companies, the economic loss is constrained.

Focus on Asia

Asia is the third most impacted region in the scenario with economic losses ranging between $6-19 billion. The region is less affected than the US and Europe due to a lower presence of sectors with high vulnerability scores, thus less likely to be infected.[1]

The healthcare, transportation and manufacturing sectors are the most severely affected sectors in the region. The disruption to production lines halts or slows down production in manufacturing companies across Asia. Countries such as China, which has the second largest share of total intermediary goods exported in the world, are particularly impacted in the scenario.

The disruption to transportation links compounds the economic loss in the manufacturing sector as stocks of final and intermediary goods already produced are forced to remain in storage.

Global 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, Cyber Extortion, Incident Response Costs, Personal Cyber along with Liability. The total claims paid by the insurance industry in this scenario is estimated to be from $10 billion in S1 to $27 billion in X1 (where the loss of data from the malware triggers additional claims of data and software loss).

Close examination of these results indicates that Business Interruption coverage is the main driver of the insured losses (71% of total losses for S1, 59% for X1).

A comparison of the insurance losses with the total economic losses and the 2019 estimated total global cyber insurance premium puts these losses in context. Comparing the insurance loss estimates to the economic losses shows insurance industry losses are between 9% and 14% of the total economic loss, which shows there are high levels of underinsurance for this type of cyber-attack.

The estimated 2019 cyber affirmative insurance premium globally is $6.4 billion, which puts the insurance industry loss estimates at 1.2 to 3.4 times the annual insurance premiums. [2] This shows that the insurance industry is significantly exposed to a contagious malware event.

[1] A Sectoral Vulnerability Score (SVS) was created by CCRS to capture and integrate the key components of sectoral vulnerabilities to malware. The companies with more severe and frequent historical malware events and those with lower defensive capabilities are scored to be more vulnerable. Please see Section 3 for more information.

[2] This is calculated by summing all the losses minus the non-affirmative Business Interruption losses and dividing by the estimated 2019 cyber affirmative insurance premium.

Types of companies that would make claims

There are three primary categories of policyholders that would make claims in this scenario:

1. Companies directly impacted by ransomware attacks in sectors highly dependent on connected and IT devices for revenue.
    a. Business Interruption due to the unavailability of IT systems or data resulting in loss of profits and extra expense.
    b. Data and software loss for reconstituting encrypted and wiped data.
    c. Cyber extortion loss for ransom payments.
    d. Incident response costs.
    e. Liability, which covers the cost of claims resulting from the cyber incident.
2. Companies indirectly affected - those companies not affected by the ransomware attack but are impacted by third-party IT failure and supply chain disruption.
    a. Contingent Business Interruption.
    b. Liability, which covers the cost of claims resulting from the cyber incident.
3. Defendant companies.[3]
    a. Liability and Technology Errors & Omissions resulting from third parties, inadequate technical services or products.

Conclusions

The report shows that the reliance of the global economy on connectivity significantly increases the scope of the damage caused by malware and, for the first time, quantifies the impacts of a global, systemic, ransomware attack.

Many sectors would be affected across the world with the largest losses in retail, healthcare, manufacturing, and banking. The impacts spread throughout the supply chain caused by the encryption of digital devices with contingent business interruption identified as particularly damaging. For example, indirect losses in the banking and finance sectors would roughly match the direct economic impact of the malware for that sector.

The scenario challenges assumptions of global preparedness for a cyber-attack of this nature and sends a clear message to organisations – individual entities, industry associations, markets and policymakers – that they must improve their awareness, and assessment of this threat.

This includes building effective response capability to contagious malware as a key part of their business operations and working more closely with insurance companies to develop cyber defence strategies.

There are also lessons for the insurance sector, as the report also highlights potential insurance policy, legal, and aggregation issues in cyber insurance offerings. Insurers should make explicit allowance for aggregating cyber-related catastrophes. To achieve this, data collection and quality is important, especially as cyber risks are constantly changing.

There are also opportunities for insurers to grow their business in the insurance classes associated with ransomware attacks. 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.[4] The increase in cyber-attacks in 2017 in Asia over recent years means companies are more likely to have standalone cyber insurance than before. Further insurance take-up is likely in the future.

The US is the world's most developed cyber market and one that is growing year on year, while in Europe, GDPR legislation and its penalties for non-compliance should stimulate further growth in the market.

The expansion of the cyber insurance market is both necessary and inevitable. Scenarios such as the 'Bashe Attack' help insurers expand their view of cyber risks ahead of the next event and help them create new products and services that make businesses and communities more resilient.

[3] The scenario assumes that a limited number of companies directly impacted will sue their IT service providers who fail to provide services due to outages in their systems, and whom companies deem as culpable in not protecting their systems from malware vulnerability.

[4] Williams 2016; Weinland 2017; OECD 2017