CyRiM Report 2019

Bashe attack

Global infection by contagious malware

Nanyang Technological University Singapore

Lloyd's

Aon

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 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 the 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 $6-18 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 band 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

1. Introduction to the scenario

1. Introduction to the scenario

The 'Bashe attack: Global infection by contagious malware' scenario was created by the University of Cambridge Centre for Risk Studies (CCRS) as a fictionalised account of a catastrophic global cyber-attack through malware infection. It presents an unlikely, and extreme, yet plausible scenario that culminates in catastrophic economic and insurance losses with lasting consequences. The scenario narrative is informed by research into historical precedents and consultations with subject matter experts to ensure consistent validity and realistic conclusions.

With inherently global economies becoming progressively dependent on digital links, it is essential to understand the strengths and weaknesses of these links. Technology has improved resilience to countless threats from an individual level to a societal level. However, increased dependence on connectivity exposes a new breed of risks.[5] The instant communication and security involved in international trade, electricity, gas, oil, air traffic, road and railroad networks are all highly dependent on process control and networked computer systems[6] and each has the potential for manipulation in a cyber-attack.[7]

The Bashe scenario

Box 1: Bashe attack

In literary usage, Bashe is found in the Chinese four-character idiom '*bashetunxiang*' 巴蛇吞象, which gives its lore of a giant "ba-snake gulping down an elephant", a metaphor for a being who is "inordinately greedy or extremely insatiable". This name has been adopted for the attack in this scenario as it is seemingly insatiable in its quest for disruption.

To depict a range of impacts for the Bashe attack, CCRS developed three scenario variants, each with an increasing degree of severity.

The S1 scenario represents a low probability, high impact set of consequences for a ransomware attack that encrypts the data on infected devices running Operating System A, compromising 43.1% of all global devices. The S2 scenario presents a significantly worse assumption set where the encryptor has the capability to impact devices on both Operating System A and B totalling 97.3% of all devices worldwide. In the X1 scenario, the malware is an encryptor for company devices and back-up wiper that can impact devices running Operating System A or B, once again totalling 97.3% of devices worldwide. The loss of data in the X1 variant changes assumptions regarding regulatory payments, exclusion clauses, and the lines of insurance impacted. The X1 scenario represents the credible upper extreme of the permutation of variables and would equate to the 95th percentile of confidence.

The extended scenario narrative of Section 2 details the events and effects of the S1 scenario where the ransomware encrypts the data on infected devices. While an extended narrative is not provided for the S2 variant, which increases the susceptible population, or the X1 variant where the malware encrypts the data and wipes the back-ups, the results for economic and insured losses are detailed for all three variants.

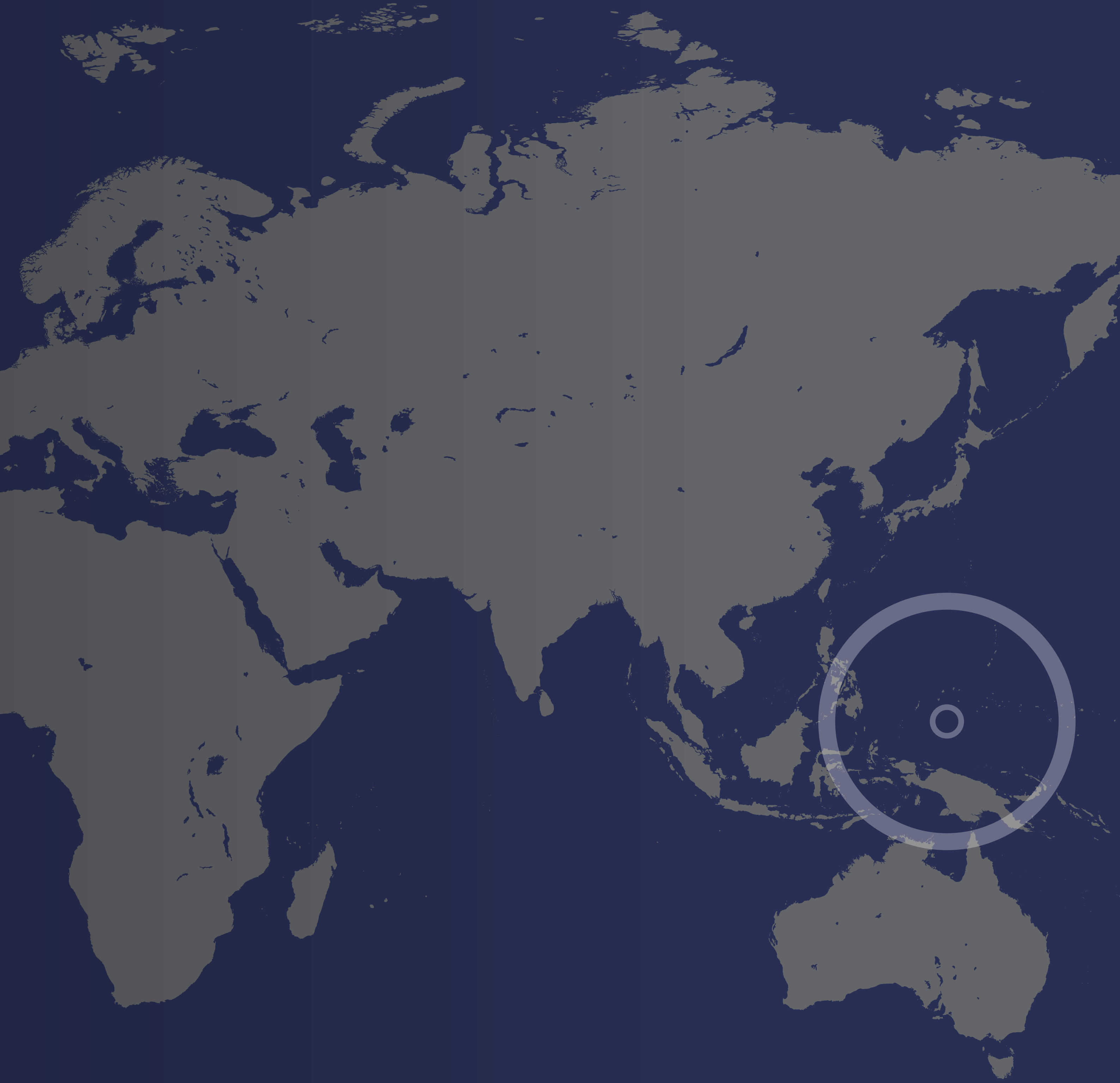
Scenario creation and interpretation is an exercise in understanding the holistic effects of a catastrophic event. The narrative outlines a series of events leading up to, during, and following a global ransomware attack to provide useful insights for the insurance industry without supplying highly securitised and essential vulnerability information or systemic flaws to would-be attackers. The Bashe scenario is offered as a stress test to challenge the assumptions of the status quo regarding cyber preparedness and to enable companies to benchmark their risk management procedures. It raises awareness of a systemic threat to all companies that rely on connected devices for management and revenue. In addition, the analysis of this report highlights potential insurance policy, legal, and aggregation issues in cyber insurance offerings.

[5] Dickey 2015

[6] Gottwald 2009

[7] Ruffle et al. 2015

2. Bashe attack: Global infection by contagious malware scenario

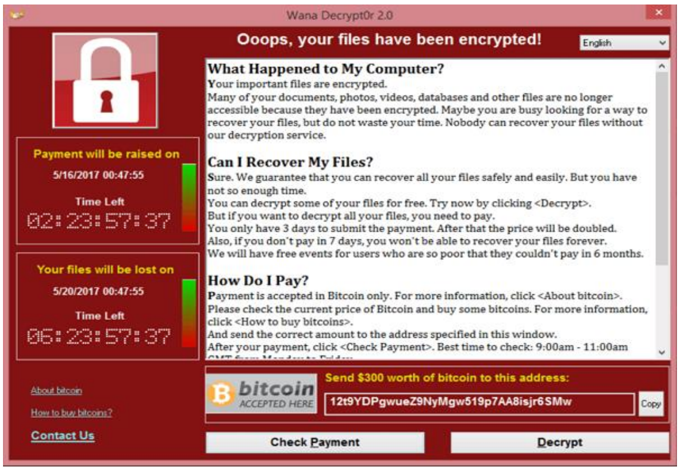


2. Bashe attack: global infection by contagious malware scenario

The continued growth and reliability of cryptocurrencies motivates an established crime organisation in southeast Asia to move into the cyber sector of the black market. The organisation's offline ventures provide the capital required to source a team of highly educated and experienced professionals to design the most disruptive malware event to date, ransoming millions of devices across the globe within minutes.

Phase 1: Recruitment

The process of vetting and recruiting takes six months before all members of the team have signed their contracts and begun. Following consultations with members of the black economy and IT professionals, the venture determines its team requires six programmers to carry out a malware attack on a global scale within the year. To ensure a profitable operation, all members of the team are given a 2% stake in the profit from the attack. All members are fully aware of the purpose of their employment.



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

The Wanna Decryptor ransomware note[8]

Phase 2: Research and development

The destructive nature of the attack and the potential for substantial financial reward makes a global ransomware attack alluring to all members of the team. They know that to reap a significant sum their attack must target a significant number of devices, be able to spread independent of human interaction, and successfully encrypt all essential data on the affected devices. The attack team strategically avoids the pitfalls of previous global ransomware attacks, which have included a web-based kill-switch (WannaCry, 2017),[9] the mishandling of bitcoin addresses to each device (WannaCry, 2017),[10] and attacking a vulnerability with a patch (WannaCry, 2017; NotPetya 2017)[11].

[8] Wikipedia 2017

[9] Newman 2017

[10] Vanderburg 2018

[11] Nunnikhoven 2017

Box 2: WannaCry - one ransomware, two perspectives

The WannaCryptor ransomware spread across the globe and infected more than 300,000 devices in 150 countries through file-sharing protocols in outdated Windows XP and Windows 8 operating systems.[12] These vulnerable operating systems were exploited across all sectors. The UK healthcare sector was crippled, causing the diversion of ambulances, cancelled appointments, and the closure of a handful of surgeries. Denial of access, or restricted access, to operational technologies, including manufacturing processes, gas pump payment applications, and telephone exchange equipment, caused an estimated $8 billion loss to businesses.[13] From a victim business perspective, WannaCry was a successfully disruptive event.

The WannaCry attackers targeted an out-of-date version of a popular operating system that already had a patch available, limiting themselves to only unpatched devices – approximately 0.1% of the 400 million eligible.[14] The ransomware demanded between $300 and $600 for the decryption key per device but lacked the ability to track payments, rendering paying the ransom useless, and the attackers earned less than $150,000 through ransom payments.[15] The purchasing of a $10.69 domain name, referenced by the ransomware, successfully halted the spread. This obstacle could have been easily avoided if the attackers had registered the web-based kill-switch.[16] Consequently, from a cybercrime perspective, WannaCry was a failure.

Phase 3: The spread

The ransomware is designed to be the most infectious malware of all time in terms of the number of companies infected as well as the number of computers infected within each company.

The malware is delivered to each company through a phishing email appearing to have come from the specified company's Payroll department with the subject 'Year-End Bonus.' The sophisticated malware mimics the domain of the target email address, using that to spoof the 'sent from' part of the email header and email address. An attachment titled 'BonusScheme.pdf' holds the trigger for the ransomware.

Once a single employee has opened the attachment, a hidden executable runs on the computer, downloading the ransomware worm. Minutes after the attachment is first opened, all data on computers sharing the network with that device have been fully encrypted and the victims are presented with a ransom message demanding $700 in an open-source cryptocurrency for decryption.

To further its spread to other networks within a company and to connected external organisations, the worm forwards the malicious email to all contacts within infected devices' address books eluding detection through its sophisticated domain mimicking capabilities. Due to its launch from an infected attachment, the majority of infections begin on desktop computers. The worm thus spreads laterally within each network of a company and continues to infect other companies and isolated networks by forwarding on the infected email. The attack is set to deploy just prior to the New Year to impact sales for the global holiday seasons and lead corporations into the new year in disarray.

Corporations regardless of size and sector find themselves in a panic as they are no longer able to process hard payments, communicate between sites via email, or run essential programs. Traders, police officers and healthcare professionals alike find themselves forced to revert to pen and paper to complete their daily duties. Infections are concentrated in sectors where connected devices are embedded in their critical infrastructure and revenue strategies.

In 24 hours, the ransomware encrypts the data on nearly 30 million devices worldwide.

[12] Graham 2017; Brandom 2017

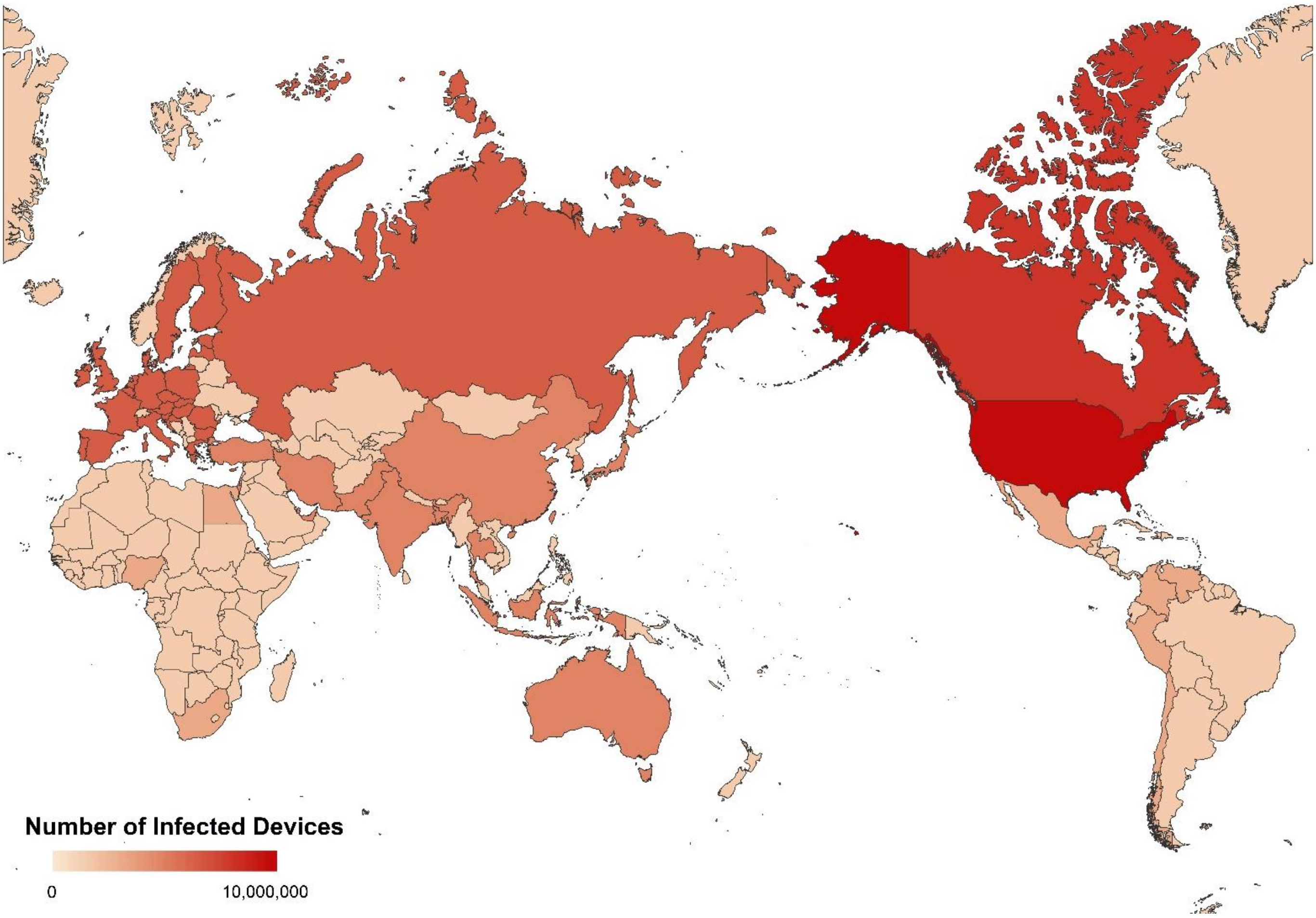
[13] "Re/Insurance to Take Minimal Share of $8 Billion WannaCry Economic Loss: A.M. Best - Reinsurance News" 2017

[14] Woo 2017

[15] Gibbs 2017; Collins 2017

[16] Greenberg 2017

Figure 1: Global infection of the contagious malware



Regardless of the rate of infection within a company, individuals and corporations are advised by governments across the world to immediately shut down all devices connected to the internet to quarantine the spread of the ransomware. This strategy has little impact as the infection spreads across the globe before the advice is given. Companies that shut down their computers in time or that run on a different operating system remain free from infection. Forced shutdowns do, however, prevent some companies from taking stock of which computers have been infected, forcing the eventual replacement or servicing of all computers on the network, regardless of infection.

Phase 4: The response

Affected companies calculate the cost-benefit of paying the ransom to avoid costly business interruption. Companies adopt a range of strategies in the days following the attack including the following:

Replace

Companies with air-gapped backup systems pay to clean up or replace all their infected devices and rely on the backups rather than pay the ransom.[17] The estimated clean-up cost per device is $350 with an average of three devices per employee including work computers, laptops, and other mobile devices.

Replacing all the computers within a network takes several days, in part due to surging demand from many impacted companies.[18] After all the computers have been replaced, employees are restricted from sending emails until further notice and internet usage is highly regulated.[19]

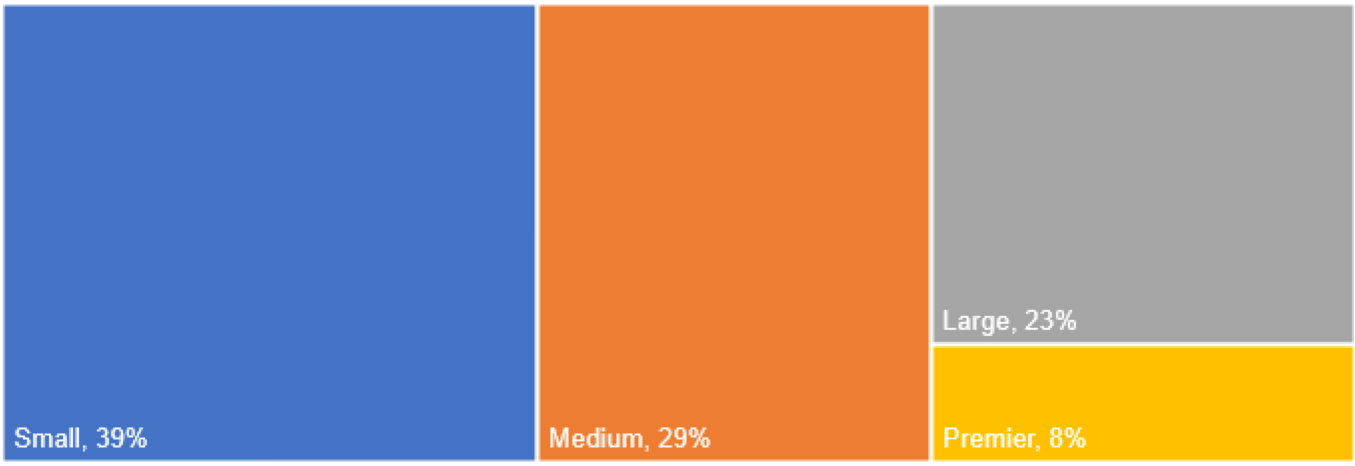
Ransom payment

Devices are successfully decrypted when the $700 ransom per infected computer is paid to encourage other companies to decrypt devices rather than replace them. Due to the critical reliance on systems, thousands of companies pay the ransom to regain access to their computers, 8% of all healthcare companies are forced to pay the ransom to keep life-saving equipment online. Similar proportions of companies pay the ransom across all sectors to reduce business interruption. Overall, the criminal organisation brings in $1.14 to $2.78 billion in extortion costs, depending on the scenario variant.
The probability of ransom payment is inversely correlated with company size. The highest proportion of companies that pay the ransom are small companies, as depicted in Figure 2. This is due to the lessened capacity of small companies to finance and manage the clean-up process combined with a lower resilience to revenue shocks, which scales up with company size. Due to potential reputation damage and financial security, premier companies are the most reluctant to pay the ransom. These companies often have the relative IT and economic capacity to deal with large-scale cyber-attacks.

Box 3: Maersk replaces tens of thousands of computers

The NotPetya ransomware attack in 2017 hit the world's largest container shipping company, A.P. Moller-Maersk. The IT team reinstalled over 4,000 servers, 45,000 PCs, and 2500 applications over a ten-day period. This was estimated to cost Maersk up to $300 million.[15]

Figure 2: Proportion of companies that pay the ransom by size and turnover[20]



[17] Osborne 2018

[18] Greenberg 2018

[19] Chirgwin 2018

[20] See Table 2 on page 19 for companies' definition. The differentiation by size of company is defined by the total number of employees and revenue.

Phase 5: The aftermath

The full extent of the damage from the ransomware attack becomes apparent and servicing the infected machines is accomplished over the course of the next year with critical systems receiving immediate attention. The global cost of the malware clean-up quickly reaches billions of dollars.

As companies slowly come back online, the media perpetuates feelings of distrust in connected devices and the imminent fear of a copycat attack. Corporate email accounts are scrutinised. Restrictions are placed on employee accounts, limiting those able to send and receive messages to external networks, changing the face of online client relationship management and business-to-business interactions.

The demand for IT security companies to assess and protect corporate networks grows exponentially in the hopes of preventing a follow-on attack. Companies across sectors and size act to better educate their workforce about cyber security. Cyber crisis management courses become an insurance requirement to ensure corporates are doing their due diligence to prevent another attack.

Some corporates may experience lawsuits against their directors and officers for their failure to prevent, and any mishandling of, the cyber-attack, causing a share price drop and a potential violation of the directors' and officers' fiduciary duty owed to shareholders. This is an added expense for corporates on top of the mounting costs of recovering from the malware event.

Once all critical systems have been restored and businesses return to near-normal functioning in the post-ransom period, focus shifts from triaging the attack to understanding it. Efforts are made worldwide to understand both the malware and its range of infection. Eventually, through flaws in cryptocurrency anonymity, the malware is traced back to the servers that were connected to an open-source cryptocurrency transaction for ransom payments. While investigators can place the servers at the time of the attack in southeast Asia, the physical hardware is no longer in existence and the attack cannot be traced.

A global push for punishment for cybercrime puts pressure on international legislation to police cybercrimes and cryptocurrency transactions. Political leaders and business professionals aim to work together to prevent another cyber-attack of such magnitude. Governmental regulations require cyber crisis management plans, employee training for cyber security, and air-gapped backups for any company connected to the internet.

3. Scenario variants

3. Scenario variants

To depict a wide range of impact for the catastrophic scenario, the Centre for Risk Studies (CCRS) developed three severity variants for the 'Bashe attack: Global infection by contagious malware' scenario.

The S1 scenario variant represents a low probability, high impact occurrence using the 'best estimate' assumptions of consequences. The S2 scenario variant presents a significantly worse assumption set. The X1 extreme scenario variant represents the credible upper extreme of the permutation of variables for S1 and would equate to the 95th percentile of confidence. It does not, however, represent the upper bound for potential losses.

The full narrative described for the Bashe scenario details the S1 baseline scenario. Although all scenario variants are highly unlikely, this variant presents the most probable sequence of events. S2 and X1 see changes made to specific variables within the set of events – the ransomware's attack surface, infection rate, and payload – which increase the damage and global impact. Internal replication rates faced by infected companies[21] remain constant across scenario variants and range between 0-50%, depending on the sector. All other variables are also held constant across these variants.

A key aspect to determining the characteristics of the scenario variants was the CCRS Historical Malware Dataset and Malware taxonomy. CCRS compiled historical malware precedents dating from 1988 to 2018 including data on all aspects of the attacks including but not limited to infection rates, replication rates, operating systems, file types, damage costs, and aliases of the malware as well as extensive interviews with subject matter experts.

This internal dataset allowed CCRS to create low probability, but technically sound, scenario variants founded on historical occurrences as is done in natural catastrophe scenario modelling.

Overview of scenario variants

Table 1: Scenario variants with key statistics

Scenario variant	Attack surface	Range of infection rates[22] *% of companies infected by size*	Payload
S1	Operating System A	1% - 9%	Ransomware for all network devices
S2	Operating Systems A and B	2% - 16%	Ransomware for all network devices
X1	Operating Systems A and B	3% - 21%	Ransomware for all network devices and a Wiper for all backups

[21] Companies in this report refer to private sector only. Public institutions are excluded from calculations, but would likely be exposed.

[22] The infection rates shown in Table 1 represent a range that has been scaled based on a Sectoral Vulnerability Score, described further in this section.

Attack surface

The attack surface is defined as the number of devices vulnerable to an attack. In this scenario set, the number of devices vulnerable to attack is dictated by the targeted operating system. To increase the severity of impact for each variant, the attack surface is extended.

For the S1 scenario variant, the attack surface is restricted to those devices running Operating System A, which runs on 43.1% of global devices.

For the S2 and X1 scenario variants, the wider attack surface includes devices using both Operating Systems A and B. Operating System B encompasses 54.2% of global devices. The combined total of these two operating systems thus increases the potential attack surface to 97.3% devices worldwide.

Infection rate

The infection rate is defined as the number of companies impacted by the attack. While cyber threat actors intend to infect all potential companies, the proportion of companies that suffer from the infection is much lower due to diversified company IT security configuration. In each variant of the attack, the ransomware becomes more effective, infecting more companies across scenario severities. The differentiation by size of company is defined by the total number of employees and revenue as outlined in Table 2.

Table 2: Size of companies for use in the Bashe scenario

	Number of employees		Revenue	
	Typical Min	Typical Max	Typical Min	Typical Max
Premier	>2000		>US$3 Bn	
Large	500	2000	$40 M	$3 Bn
Medium	100	500	$10 M	$40 M
Small	20	100	$2 M	$10 M

Source: Managing Cyber Insurance Accumulation Risk, CCRS and RMS (2015)[23]

The historical precedents of infection rates from ransomware delivered by phishing in the CCRS Malware Dataset and Malware Taxonomy combined with subject matter expertise resulted in the infection rates detailed in Table 3 which details the baseline infection rate by size of company for each of the scenario variants. These infection rates were differentiated by sector using a Sectoral Vulnerability Score (SVS) created by CCRS shown in Table 3.

The SVS score attempts to capture and integrate the key components of sectoral vulnerabilities to malware. These components are operationalised as historical precedents and current defensive capabilities. Those companies with more severe and frequent historical malware events and those with lower defensive capabilities are scored to be more vulnerable. This score ranges from 1 to 5, with 1 indicating the most secure sector with strong defensive capabilities and a lower likelihood of being infected by malware and 5 indicating the least secure sector with the weakest defensive capabilities and a high likelihood of infection.

[23] "Managing Cyber Insurance Accumulation Risk" 2016

Table 3: Infection rate by size and sector for S1

Sector	SVS	Premier	Large	Medium	Small
Business & Professional Services	3	4%	3%	3%	4%
Defence / Military Contractor	1	3%	3%	3%	2%
Education	5	9%	6%	6%	8%
Energy	2	5%	2%	2%	3%
Entertainment & Media	4	7%	4%	4%	5%
Finance - Banking	5	7%	6%	6%	8%
Finance - Insurance	4	6%	4%	4%	5%
Finance - Investment management	4	6%	4%	4%	5%
Food & Agriculture	2	3%	2%	2%	3%
Healthcare	4	6%	4%	4%	5%
IT - Hardware	4	7%	4%	4%	5%
IT - Services	4	7%	4%	4%	5%
IT - Software	4	5%	4%	4%	5%
Manufacturing	4	5%	4%	4%	5%
Mining & Primary Industries	1	4%	1%	1%	2%
Pharmaceuticals	1	4%	3%	1%	2%
Real Estate / Property / Construction	4	6%	4%	4%	5%
Retail	5	8%	6%	6%	8%
Telecommunications	2	4%	3%	2%	3%
Tourism & Hospitality	3	5%	3%	3%	4%
Transportation / Aviation / Aerospace	4	5%	4%	4%	5%
Utilities	2	4%	2%	2%	3%

An overall look at the infection rates of companies in the Bashe scenario finds the highest rates of infection at the ends of the spectrum in premier companies with 2000+ employees and small companies with less than 20 employees as these two company sizes have opposing attributes on two of the key components for determining infection rates: Company Size, and IT contributions.

As stated, one of the key components for the infection rate is the size of the company by the number of employees, as those companies with more employees have more access points into their company networks from external sources. The infection rate for premier companies is thus higher compared with medium and large companies as the attack surface for threat actors to exploit is significantly greater in terms of the number of internal employees, and those connected by third party vendors in a supply chain. Although Premier companies are more likely to have dedicated IT personnel and training, insider threat continues to be responsible for the greatest number of incidents within a company.[24]

The lack of significant budgets or contributions of the IT personnel and training counteract the reduced points of entry in small company networks.

On average, small companies, when adjusted for size, have lower IT spend, and training with less resources dedicated to IT security increasing their infection rates comparably to that of premier companies.

To increase the severity of each scenario variant, the worm infects more companies worldwide with each iteration. For the S2 variant, the ransomware can attack roughly twice as many machines in S1; Operating System A and Operating System B are now both susceptible to the attack. As such, the infection rate also roughly doubles, with some deviation due to SVS. For the X1 variant the infection rate increases by an additional 35% from the infection rate of S2, with slight deviations by sector due to SVS.[25] The driver of this increase is that the threat actors adapted their phishing delivery mechanism which increases the volume of malicious emails sent across sectors but does not overload Border Gateway Protocols or Internet Service Providers. The higher volume of emails sent increases the likelihood of infection. An additional behavioural assumption is made in the X1 scenario that employees in companies are on average more susceptible to phishing emails. This results in an increase in the number of successful infections.

[24] Schick 2017

[25] Please see the ‘Guide to Portfolio Loss Estimation’ (Appendix) for details on S2 and X1 infection rates.

Replication rate

The replication rate is defined as the number of devices within a company that are infected. The more devices affected within a company, the greater the disruption to the company's continuity. Each sector in the Bashe scenario is assigned a distribution of internal replication ranging from 0%-40%+[26] based on the Sectoral Vulnerability Score (SVS).

Those sectors with a higher SVS have more companies that suffer greater internal replication of the malware and thus more disruption. Internal replication rates increase with increasing vulnerability scores. For example, 35% of sectors with a vulnerability score of 1 are subjected to a replication rate between 0 and 10%. The distribution of replication rates was derived from the CCRS malware taxonomy and remains constant across the scenario variants. It is important to note, however, the absolute number of computers infected varies across the variants as the spread of the ransomware internally is conditional on the infection rate.

Table 4: Distribution of replication rates by vulnerability

SVS	0-10%	10-20%	20-30%	30-40%	40%+
1	35%	45%	10%	7%	3%
2	30%	42%	10%	12%	6%
3	25%	39%	10%	17%	9%
4	20%	36%	10%	22%	12%
5	15%	33%	10%	27%	15%

Payload

The malware payload indicates the effect on the system that is infected.

In this scenario, the payload of the infection influences the degree of damage done within a company and the lines of insurance that will be triggered. For S1 and S2, the modelling reflects a ransomware payload. In the extreme X1 scenario, the payload of the malware is a ransomware and back-up wiper, which also deletes backup files on the infected network.

Computers infected with ransomware (S1 and S2) have their files on the ransomed device, and all other files on the connected network, encrypted. Once the computer has been forensically cleaned, the device is usable again as the backups for the device are not affected. If a decryption key is found, or the ransom is paid, the data on the device can be fully recovered. The increased losses from S1 to S2 are due to increased infection rates globally and increased attack surface.

Computers infected with a ransomware and back-up wiper (X1) have the files on the network encrypted and backups for the devices deleted permanently. While the devices themselves can be reused once they are reconfigured, infected companies incur permanent damage from the wiped data.

Table 5: Payload potential disruption[27]

Payload Type	Definition	Severity
DDoS	Malicious attempt to disrupt normal traffic, server, or network by overwhelming infrastructure with a flood of internet traffic	🟩
Credential Stealer	Steals private and personal information from infected systems	🟨
Bot & Botnet	Take control of computers and organise infected machines into networks of bots that a criminal can remotely manage	🟨
Ransomware	Blocks/encrypts access to data unless a ransom is paid	🟧
Wiper	Wipes and overwrites the hard drive or permanently randomises data	🟥

[26] CCRS completed extensive research on worm propagation and found that worms have an upper limit of propagation within internal networks. After consulting with subject matter experts, the most accurate upper bound for infection was decided to be 40%+ to remain technically feasible.

[27] CCRS developed a methodology to assign a severity score to broad categories of payloads. We define payload severity as: the cost to the user of an individual device due to the execution of a given payload. The attributes of the payload used to determine the potential severity include: objective of payload, detectability time of the payload in a given system, and the duration of removal time from that system.

4. Direct impacts on the economy

4. Direct impacts on the economy

In S1 over 250,000 companies worldwide are impacted by the Bashe Ransomware. In this section, the effects of the encryption are illustrated at a primary sectoral and primary aggregate level to demonstrate the depth of impact. The secondary effects follow on from the aggregate primary effects with lasting long-term effects changing the cyber security landscape of the future.

Primary sectoral effects

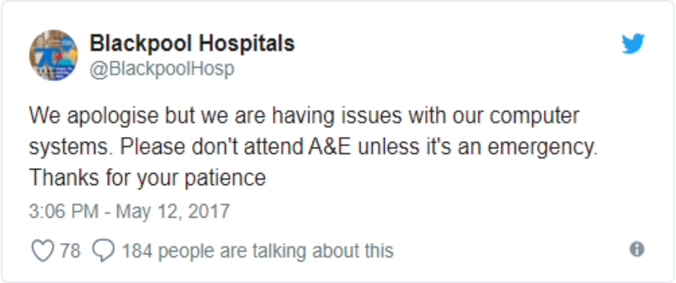
Finance

Some commercial banks, credit unions, and insurance companies are hard hit in Financial Services, incurring large financial losses from service disruption. Several banking services are disrupted, and some computer systems are shut down, causing widespread infrastructure damage and, in more extreme cases, global chaos in financial markets. Digital banking portals are affected for several days as customers are unable to make payments or perform simple activities such as checking their balances, and the risk of fraud increases. Because of this banks then waive overdraft fees and increase interest rates to avoid losing customers unable to access accounts. A broker-dealer subsidiary of a systemically important banking organisation is unable to enter buy or sell orders in trading which renders them unable to pay checks or debits, honour their derivative transactions, respond to margin calls, or transmit or receive cash to pay principal. If an organisation has insufficient emergency response plans and is unable to recover in a period of a few weeks it may become unable to perform its legal obligations as it becomes overwhelmed due to requests from customers and counterparties, subsequently falling into default and triggering an orderly liquidation to bolster tumbling public confidence. Directors and officers (D&O) liability insurance lawsuits may begin for listed companies with poor response and disaster recovery plans.

The various regulatory requirements and organisational complexities of the Finance sector lead to a range of results, many of which will be unanticipated.[28]

Healthcare

The ransomware enters healthcare networks via email, extending to the software programs customised for specialised use by the medical industry. The infected medical practice management and clinic management software no longer allows practitioners (administrative staff, nurses, doctors, emergency response units) to view and share patients' medical histories, make notes about their current conditions, and issue prescriptions. The ransomware attack disrupts these critical activities, encrypting this private and crucial data and making the treatment of many patients impossible. In some cases, data is lost entirely.[29]



Blackpool Hospitals
@BlackpoolHosp

We apologise but we are having issues with our computer systems. Please don't attend A&E unless it's an emergency. Thanks for your patience

3:06 PM - May 12, 2017

♡ 78 184 people are talking about this

Clipped tweet from the Blackpool Hospital Twitter page on 12 May 2017

The malware spreads into networked devices that may be reliant on Operating System A, such as diagnostic imaging devices, image archiving, and data capturing systems. Patients are diverted to other practices, overwhelming their response teams. The relocating of emergency cases incurs heavy costs as road and air ambulance services are deployed. Appointments are cancelled, leading to medical liability claims from patients who feel unfairly treated.

[28] Glassman and Miller 2016

[29] Kearney 2018

For some General Practitioner (GP) practices time-tracking and payroll systems within healthcare are impacted, shutting down operations at even the most basic levels. Uninfected GP practices are impacted by taking their systems offline to avoid infection and by the increase in patient referrals from affected practices, causing business workflow disruptions in hospitals.

In the most extreme cases, some patients may die from not being able to receive emergency or adequate treatment or having their treatment delayed as they are transferred to an unaffected facility.[30]

Box 4: WannaCry hits the NHS[30]

On 12 May 2017, the National Health System of England alerted the Department of Health and Social Care that 16 trusts had suffered ransomware attacks, declaring a major incident and initiating its emergency response plans.

The attack lasted one week. Five acute trusts providing hospital services had to divert operations as they experienced issues with diagnostic services including MRI and CT scanning technologies. Elective procedures were cancelled. Services that were not infected were also impacted as they took email offline to reduce the infection risk. 8% of all GP surgeries were impacted and one third of hospital trusts in England were disrupted. 139 appointments were re-arranged for patients with potential cancer, representing 0.4% of urgent cancer referrals.

595 infected practices required their machines to be rebuilt before they could be patched, each involving an in-person visit from a technician. The total loss to the NHS is estimated at £92 million.

Transportation

The internal computer systems for public transportation services are affected, disrupting ticketing systems and forcing public transport networks like bus and rail services to offer free services to customers. Kiosks used by customers go offline, resulting in travellers seeking out other modes of transport, causing traffic jams on arterial routes as the number of commuters in cars and on the streets spikes. Replacement bus services are offered, contributing to the congestion and lost cost. Airports experience minor disruption to their business operations as ticketing systems are temporarily disrupted.

In more extreme cases, some flights may be cancelled regardless of infection as fear of widespread system compromise mounts. Administrative systems are impacted, and applications are taken offline as a precautionary measure to protect more critical systems. For airports where flights are not cancelled, operators revert to manual processes such as whiteboards to keep passengers informed of flight times.[31]

Retail and Hospitality

Several e-commerce sites experience site delays and service interruptions as their service providers are affected by the ransomware, shutting down some components of their websites. Online consumers visiting the impacted sites are faced with an increase in error messages and difficulties, causing an increase in shopping cart abandonment rates and a subsequent drop in conversion rates. Some potential consumers are locked out of their private machines, making them unable to browse e-commerce sites or complete purchases. Others reduce their computer usage and internet browsing behaviour for hours to days out of fear of infection, many at the request of their employers. A failure in some electronic means of payment affects point-of-sale purchases at brick-and-mortar stores. Restaurants and bars are especially affected, leading to long queues at cash machines as consumers hurry to draw cash to pay for services already rendered.

Information Technology

Information Technology plays a role in all sectors to varying degrees and is itself a highly diverse sector. When the cyber-attack first comes to light, technology suppliers for sectors like Finance and Healthcare are inundated with calls to find a patch for their networked devices and rebuild critical machines. Computer services struggle with the influx of requests from panicked consumers while simultaneously working on combatting the ransomware. Information services across sectors are shut down by IT teams to stop the ransomware from spreading. The combination of sectors shut down, and IT support sectors being overwhelmed with requests, leads to labour shortages in other areas, exacerbating the crisis.

[30] Smart 2018; Field 2018

[31] “Cyber Attack Led to Bristol Airport Blank Screens” 2018

Manufacturing

Manufacturers of electronic products and automotive manufacturers[32] who gather component parts from a range of third-party suppliers struggle with different levels of compromise throughout their global supply chains as their vendors place pressure on them to secure their business processes. Mass product recalls are triggered to avoid liability lawsuits and salvage consumer trust[33] and the cost of materials spike due to shortages and delays. Uninfected tangential support systems are temporarily shut down amidst fears of related intellectual property theft, stalling production.

Box 5: 500,000 Pacemakers recalled[33]

The FDA identified critical security holes in six types of pacemakers made by healthtech firm Abbott and sold under the St Jude Medical brand. Half a million patients with these pacemakers required a firmware update by a medical professional to patch the security holes.

The vulnerability would have made it possible for a malicious actor to reprogram the pacemaker and conduct "inappropriate pacing" or run the battery flat, activities that would have been fatal for the patients. Fortunately, no unauthorised access was reported before the firmware upgrade could be completed.

Primary aggregate effects

Communication

Information and communication technology (ICT) is a core reliance in most sectors, especially Finance, Information Technology, Retail, and Transportation. As the ransomware proliferates via email, companies that rely heavily on email suffer high levels of business interruption. Employees resort to other means of internal communication, primarily through mobile devices, leading to an increase in instant messaging through Facebook in North America; WhatsApp in South America, Africa, Europe, and South Asia; and WeChat in East Asia. For companies heavily reliant on email services, all operations come to a standstill. Subsidiary companies of large delivery organisations are infected, disrupting delivery and communications for their principal organisations.[34] Employees create new email accounts with different providers, creating further confusion amongst their customers.

Phone systems are disrupted, impacting companies that rely heavily on telecommunications such as in the Sales and Shipping sectors. Companies temporarily employ the use of hand-written letters and post for urgent correspondence along the supply chain and between branches. Some employees bring their personal, uninfected, computers to the office to hasten the return to business as usual, in some cases worsening the spread of the ransomware. Response efforts are delayed as technicians struggle to communicate with the infected company to assess the cause of the disruption.

Box 6: FedEx hit by NotPetya[34]

TNT Express, a subsidiary of FedEx in Europe, had its delivery and communications disrupted worldwide by NotPetya mid-2017. The resulting operational disruption cost FedEx $300 million in the last quarter of the financial year. Not all systems were recoverable following the attack. TNT Express volume, revenue, and profits had still not returned to normal levels by their year-end report.

Productivity

As manufacturers struggle with stalls to production and companies deal with high levels of business interruption, factories and offices send workers home who are unable to work and to stop the infection from spreading. Extra support staff for IT technicians are brought in to work on the incident, costing companies additional consulting fees and overtime rates for staff. The attack leads to the operational failure of organisations' network systems, leading to loss of productivity and sales, affecting retailers particularly as well as business productivity.

Trade

Delivery and maritime shipping operations are suspended, complicating efforts to load and unload ships. Delays in operations lead to mounting demurrage fines as operators struggle to issue movement orders. This leads to a cascading impact along the supply chain as perishable goods and critical goods are immovable. Levels of theft increase amidst the confusion as criminals take advantage of the chaos to profit from the operational difficulties faced with moving expensive items and electronics.

[32] Dalesio 2017

[33] Hern 2017

[34] Palmer 2017

Smart devices

The ransomware self-propagates through the network to affect smart devices running the affected software and devices reliant on computers or servers running the affected software such as wearables, thermostats,[35] order processing devices for restaurants, public digital displays, key-card gates, and healthcare devices. Effects vary but in more extreme cases lead to IT support costs to decrypt devices, replace the server or upstream operating machine, lost marketing costs, bad publicity, and loss of consumer trust in the supplier. Bars and restaurants with fully integrated order and payment Internet of Things (IoT) systems experience high levels of business interruption.

The development of smart cities is significantly hampered globally until government officials can be assured that all networks and systems have been analysed and fortified to ensure the protection of citizens.

Lloyd's worked with UCL STEaPP and the PETRAS Research Hub on the *'Networked World'* report that identified emerging risks and opportunities arising from the interconnected and increasingly ubiquitous character of the IoT.

Box 7: Casino compromised by internet-connected fish tank[35]

In July 2017, an unnamed North American casino suffered a breach of its high-roller database due to an internet-connected fish tank in the lobby. The fish tank was connected to a computer to monitor tank cleanliness, food, and temperature. This enabled hackers to enter the broader casino network, find the database, and pull that data back across the network, through the aquarium thermostat, and up to the cloud where they could access it.

Consumers / Households

Consumers have the potential to be directly impacted by the Bashe attack. Although the targets of the attack are corporates, the victims' entire address books are forwarded the malware so there is potential for individual consumers to have their personal hard drives encrypted, with some paying the ransom. Encryption of household devices may contribute to a minimal decline in e-commerce sales as owners of the infected devices are unwilling to purchase goods and services online due to a lack of trust in the security of their devices. Households will also likely have to bear the costs of replacing or cleaning the infected devices.

Secondary effects

Affected companies and consumers begin to approach technology more cautiously for a short while, especially after the large-scale financial losses suffered by industries. These dollar values are splashed across news headlines globally for months following the attack as financial statements and earnings reports are gradually released to the public and the costs are tallied. Many companies begin re-evaluating their suppliers, cautious of flaws in their reliance on third-party products and services that could bring down their own operations. Organisations use additional funds to bring in IT consultants who spend days upgrading and patching computers, industrial control systems, and other connected devices. Depending on the company, employee labour is redirected for several hours or, in some cases, days towards mandatory cybercrime-awareness training and workshops to attempt to decrease the severity of the next attack. Companies that had their communications affected, particularly in the Sales, Delivery, and Shipping sectors, consider alternative means of communication in the event of an emergency and make these plans known to partner businesses.

Long-term effects

The investigation leads security experts to the servers associated with open-source cryptocurrency payments, but the physical hardware has since been moved. The crime organisation is never identified and does not publicly claim responsibility for the attack. Companies that were affected by the ransomware go to court to waive fines from regulators for breach-of-contract cases from businesses with whom they work. Legal cases, arising due to halted services, go on for years. Some companies continue to suffer losses in subsequent years because of the attack.[36] New regulations come into effect that require information and operational technology organisations to follow certain rules regarding their approach to emergency response plans, dealing with suppliers, employee training, cyber and business interruption insurance, and software and hardware maintenance. Data sharing on cyberattacks becomes a more transparent process in all sectors, with published reports and databases containing publicly available critical information. Countries lacking mandatory reporting and adequate data protection laws[37] are put under increasing pressure to change their policies to continue participating in international trade and for the InfoSec community to obtain a more complete view of cyber activities around the world.

[35] Schiffer 2017

[36] Ralph 2018

[37] "Data Protection around the World" 2018

5. Global and regional economic losses

5. Global and regional economic losses

The negative economic consequences of the Bashe scenario are experienced across the globe. Shocks to productivity, consumption, and subsequent costs related to clean-up and extortion cause significant impacts on the revenue of companies directly affected. The interlinkage of technical and economic networks causes significant contagion effects across the globe, particularly for companies exposed through their supply chains. Economic loss is heterogenous according to company size, sector, and region - and driven by numerous economic and technical factors.

To capture the global scope of the scenario, CCRS developed an industry exposure dataset, which estimates the population of companies by size and sector in four regions of the world[38]:

- United States (US)
- Europe (including Russia)
- Asia
- Rest of World (RoW)

Using this dataset, the economic and insured loss was modelled across these regions. The total number of countries modelled within each region captures 92% of nominal global gross domestic product (GDP) in 2017. CCRS aggregated these regional results to calculate global losses for the scenario.

Categories of economic loss

Direct loss due to productivity shock

The encryption of digital devices disrupts business operations including logistics and distribution, production activities, financial transactions, and digital communications such as email. This disruption causes business productivity to decline as employees are unable to perform to an ordinary standard, causing the output of infected companies to decline. To estimate the direct revenue loss from the fall in output, the daily impacted gross revenue was multiplied by the total outage days. The percentage of revenue loss and duration of outage varies depending on loss drivers such as infection rate, replication rates, and a sectoral criticality score which measures the relative dependency of firms on connected and critical systems.[39]

Direct loss due to consumption shock

The impact of the scenario results in a decline in consumption in the short term. Encryption of e-commerce platforms and electronic payment systems disrupts the purchasing of goods and services. The impact on consumption is likely to be mitigated due to the abundance of alternative payment methods and consumers may substitute online for traditional high-street shopping.

In this scenario, it is likely that some households will inadvertently fall victim to the ransomware attack. This may result in some customers being unable to purchase goods and services due to the encryption of their devices. The impact of this on overall economic loss is likely to be minimal due to low penetration of infection in households relative to the commercial sector.

Consumption will likely return to pre-shock levels as digital service companies overcome the outage caused by the malware. However, e-commerce retail companies may suffer a more sustained shock to revenue due to the negative impact on their brand resulting from the infection.

Indirect loss through contagion effect

The scenario also causes a negative contagion effect that impacts the economic loss of global businesses. Companies are indirectly impacted through a negative shock on their supply chains caused by the encryption of digital devices.

International trade is likely to be negatively impacted due to transport disruption, which causes indirect loss to all sectors in the global economy. Maritime port operations are likely to be suspended due to an outage in their IT and inventory management systems.

[38] All companies in this data set have 20 or more employees. Microcompanies were not included in the loss calculations,

[39] Each sector in the model has a decay function of internal infection that determines the duration and severity of the business interruption across time, which has an upper bound of 30 days.

Ports will be forced to suspend cargo loading and unloading until the machines are operational and the cargo in ports is relogged. This is likely to be the case for the transport of cargo through airports and railways as well. The supply chain disruption will be compounded by the fact that companies that produce intermediary goods for other firms may be directly impacted by the ransomware. This causes production failure, reducing the supply of intermediary goods in the global market. The halt in transportation prompts a stall in production across the globe and causes a cascading impact along supply chains.

To capture the indirect impacts of the scenario, a contagion multiplier was estimated for each sector. The multiplier calculates the relative indirect revenue loss as a proportion of a sector's direct loss. The value of the multiplier was calculated by employing an input-output approach to estimate the relative indirect shock in inter- and intra-sectoral trade globally using the World Input-Output Table.[40]

Cyber extortion and clean-up losses

Other economic losses from the scenario are derived from clean-up and cyber extortion related costs. For the former, there is a cost associated with decrypting and reinstating functionality to computers infected. This results in increased labour costs as IT departments are forced to hire external staff or work overtime to remove the malware from systems. Cyber extortion costs in this context are the costs of paying the ransom.

Global economic loss estimates

CCRS developed three scenario variants in this report and calculated the corresponding global losses to illustrate a range of potential losses without setting an upper limit. The figures presented in this section are outputs from CCRS modelling. The global economic costs for each of the scenario variants and regions are detailed in Table 6. The total economic losses globally range from $86 billion in S1 to $193 billion in the extreme X1 scenario variant. Table 6 also outlines the global economic loss by sub-category.

One of the main drivers of the direct and indirect global economic losses across scenario variants is the number of premier companies infected as they have the highest potential for total revenue loss. With premier companies modelled as having over 1,500 times the daily revenue of small companies, their higher relative rates of infection have a significant contribution to economic losses. This trend reflects historical precedents of ransomware attacks where the majority of reported loss has been from large multinational companies (i.e. NotPetya's impact on Maersk).[41] In addition to greater interruption and revenue losses, the increase in the number of infected devices increases the clean-up and cyber extortion costs across the scenario variants. As Table 6 shows below the primary driver of economic loss is business interruption.

Table 6: Global economic loss estimates, $ billion

	S1	S2	X1
Number of infected global companies	250,000	501,000	613,000
Total direct economic loss	$59	$110	$133
Productivity and consumption loss	$50	$93	$112
Clean-up loss	$8	$15	$18
Cyber extortion loss	$1	$2	$2
Total indirect economic loss	$26	$49	$60
Total global economic loss	$85	$159	$193

[40] World Input Output Database n.d.

[41] Nash, Castellanos, and Janofsky 2018

Global sectoral economic loss estimates

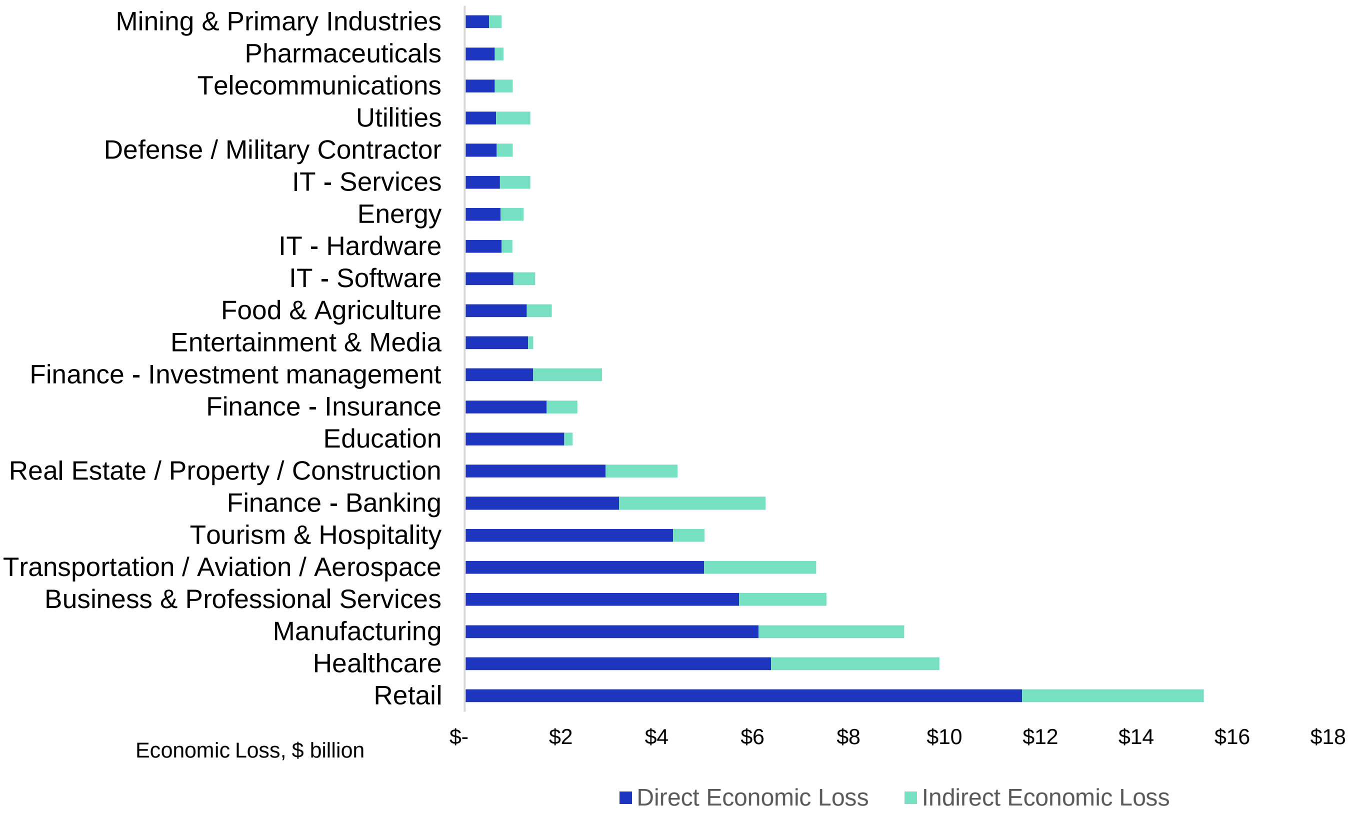
Results for the direct and indirect shocks facing global sectors for the S1 scenario variant are presented in Figure 3 (for scenario variant X1 see Annex C). Results estimate that Retail suffers the highest total economic loss globally. The encryption of payment systems in traditional retail outlets causes a significant decline in sales revenue for the duration of the outage. This can happen in two ways: a point of sale or other transaction system can become unusable or the data it stores can be encrypted or wiped, which means the vendor does not have access to the accounting records. Many vendors would choose to stop using said devices under such conditions. E-commerce retail revenue is particularly impacted as websites struggle to process web traffic and payment systems fail.

The indirect impact of the scenario on supply chain networks delays the delivery of goods and services, causing stocks to run low in the Retail industry. This causes a shortage of products in stock, which reduces sales and thus revenue. Food Retail suffers large indirect and direct shocks due to the high penetration of perishable goods likely to spoil during the outage. Healthcare is the third most impacted sector due to the penetration of legacy systems on old healthcare equipment that are difficult to clean up and patch, causing significant delays in the recovery process and increasing revenue loss. Replacing these systems also comes at a high cost. The Healthcare sector has been historically vulnerable to high levels of malware infection and replication due to a relative high penetration of vulnerable systems and low IT expenditure. Beazley reported in 2017 that there was a 133% increase in Healthcare ransomware demands.[42]

The Manufacturing sector suffers significant revenue loss due to the encryption of manufacturing equipment halting production. The encryption of inventory management systems further disrupts the production process. The indirect impact on international trade causes delays in the transportation of final goods that these companies produce and the intermediary goods required for production, further increasing disruption and decreasing revenue.

Financial services such as banking and investment management suffer significant revenue loss. The contagion effects of the scenario cause chaos in the financial markets, impacting financial institutions' investment portfolios through devaluations of financial instruments such as equities, bonds, and currency. Intersectoral contagion impact in the financial sector is likely to cause some limited liquidity issues as banks may become wary of the IT security systems of other banks, which slows down trading between banks, particularly in the interbank market.

Figure 3: S1 Total direct and indirect economic losses from business interruption by sector, $ billion



[42] Beazley 2018

Regional economic loss estimates

CCRS also estimated the total economic loss per region. Results are detailed in Table 7 below. The region with the highest total economic loss is the US, followed by Europe, Asia, and the Rest of the World.

Table 7: Total economic loss by region, $ billion

	S1	S2	X1
Total economic loss global	$85	$159	$193
US	$46	$77	$89
Europe	$30	$60	$76
Asia	$6	$14	$19
Rest of World	$3	$7	$9

Regional disparities in the economic loss estimates are caused by several economic and technical drivers. A key driver of this difference is the heterogeneity of business activity across regions. The sectoral breakdown of economic activity per region significantly influences the disparity of economic loss. As discussed in Section 3, some sectors of the economy are more vulnerable to both external and internal infection than others. This is reflected in each sector’s vulnerability score. Research into the resilience of companies to ransomware attacks found that companies in the service sectors such as Retail, Tourism and Hospitality, and Finance tend to be more vulnerable than the industrial sector (Manufacturing being the exception). This may be due to their reliance on e-commerce as a significant revenue stream. These findings were incorporated into the model, thus regional economies that are more service dominated, such as the US and Europe, suffer greater relative infection and thus direct losses.

The penetration of connected systems per sector also affects the regional impact of the cyber-attack. Sectors that have more connected systems, particularly those that are critical to the continuation of business, are more likely to suffer severe and longer shocks to revenue. This particularly impacts regions where the output of the economy is dependent on Manufacturing, Healthcare, Mining, and other primary industries.

The distribution of size of companies across regional economies also influences the severity of loss. Premier sized companies contribute significantly to economic losses for the scenario. Therefore, regions with a higher relative penetration of premier sized companies are likely to experience more severe losses.

Other technical drivers for differences in regional economic loss include: commercial device and internet penetration per region, share of global Internet of Things (IoT) devices, and penetration of third-party providers of IT services and products. These drivers influence the attack surface available for threat actors to exploit, which influences the contagiousness of the ransomware. Below is a description of the losses suffered per region.

US

In this scenario, the United States of America suffers the highest economic loss. This economic loss is primarily driven by infection of premier companies, particularly within the service sectors such as Finance, Healthcare, and Retail. High infection rates in sectors such as Finance cause a significant contagion impact to the US financial markets. Banks in the US suffer liquidity constraints in the short term as these companies attempt to re-establish their IT security after infection. The impact on banks’ liquidity trickles down to all sectors of the economy as access to accounts and loans are restricted.

A further significant contagion impact is the disruption to international trade. The US is the second highest exporter of containerised shipping in the world.[43] Ports impacted by the ransomware cause a halt in the transportation of intermediary goods. As many companies in the US have a higher reliance on marine transport for trade in intermediary goods relative to most other countries in the world, the indirect impact to sectors such as Manufacturing is particularly high.

Europe

Europe has the highest number of infected companies across the scenario variant. However, the economic loss is 36% less than that of the US. One reason for this result is that the EU has a much higher penetration of small and medium sized enterprises (SMEs) and a lower penetration of premier sized companies compared with the US. This penetration of SMEs in Europe and the relative high infection rate of small companies (due to poor relative cyber defences - see Section 3) drives the number of businesses infected.

[43] World Shipping Council n.d.

Due to the low potential revenue loss per day for small companies, the economic loss is constrained.

Europe is still severely impacted by the Bashe scenario. Retail, Business and Professional Services, and Manufacturing are the hardest hit sectors in Europe and drive much of the economic loss. The continent also suffers significant indirect economic loss due to the contagion impact of the scenario on international trade. With 50% of goods traded in the EU transported by sea, the impact of the scenario on marine ports and shipping causes a significant indirect shock across all sectors.

Asia

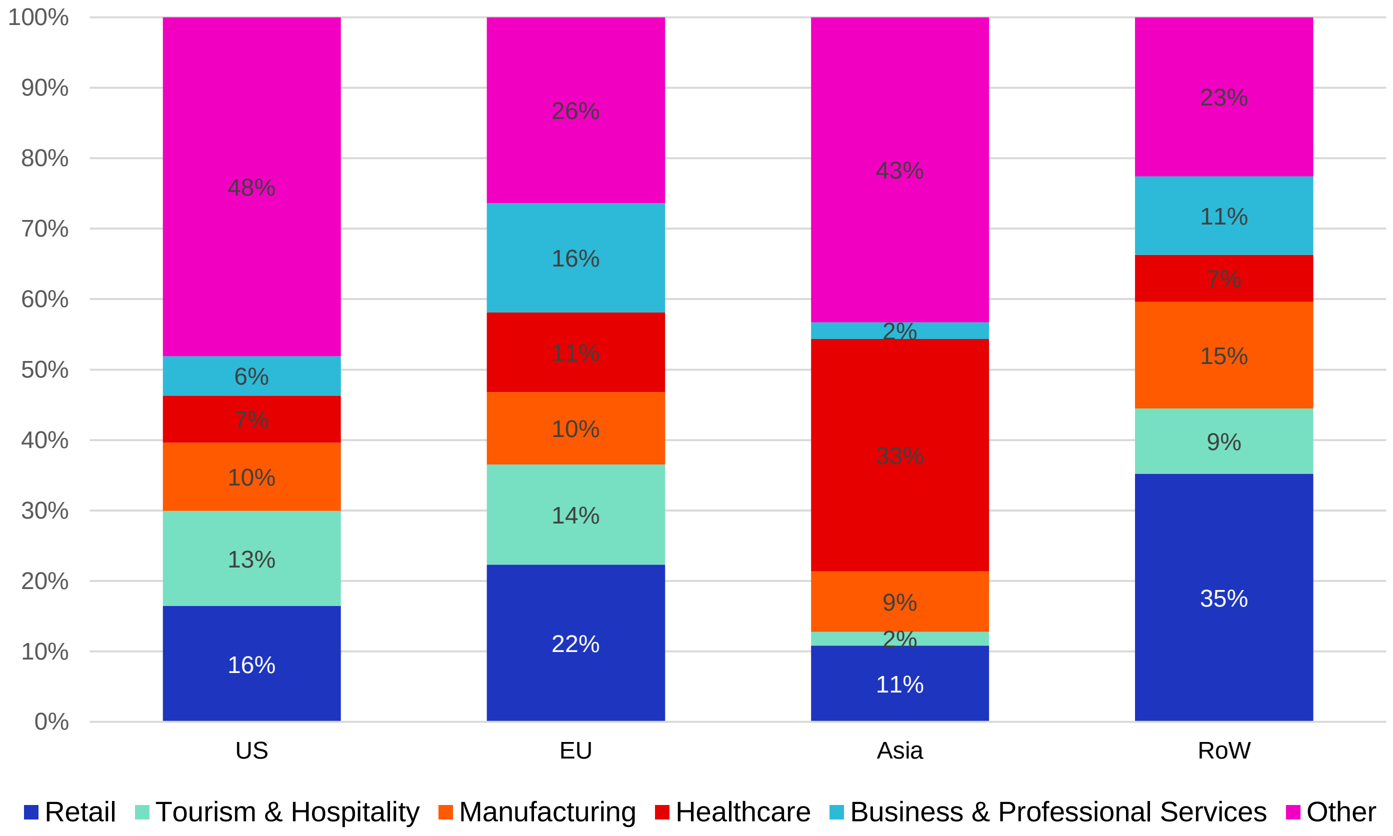
Asia is the third most impacted region in the scenario. The region is less impacted by the scenario due to the lower penetration of sectors with high vulnerability scores and thus less likely to be infected. The Healthcare, Manufacturing and Transportation/Aviation/Aerospace sectors are the most severely impacted sectors in the region. The disruption to production lines halts or impairs 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 by the scenario.[44] The disruption to transportation links compounds the economic loss experienced in the Manufacturing sector as stocks of final and intermediary goods already produced remain in storage.

Rest of world

The Rest of World is the least impacted region. This is partially due to the lower relative penetration of premier and large sized companies. One of the main mitigating factors to the spread of ransomware is the lower penetration of digital and connected systems in commercial companies.[45] The lower penetration of digital devices limits the spread of the malware, which abates revenue loss in the rest of the world. The sectors that contribute the most to economic loss are Retail, Manufacturing, and Real Estate.

Figure 4 shows the comparative overview of the direct economic losses from productivity and consumption loss in S1 by top 5 sectors and regions, accounting for approximately 85% of total direct economic losses. An overview of losses for each scenario variant is shown in Table 6.

Figure 4: Distribution of direct economic loss (productivity and consumption loss only) in S1 by sectors and regions



[44] World Bank n.d.

[45] Chinn and Fairlie 2010

Comparing loss results to historical precedent

In a matter of days, the Bashe scenario causes significant direct and indirect economic loss at a sectoral, regional, and global scale.

Table 8 compares the economic losses of the Bashe scenario to the historical precedent of the NotPetya ransomware attack across the scenario variants. The ratio of the Bashe scenario economic losses to the NotPetya attack is between 8.6 and 19.31 for the scenario variants. As mentioned in the scenario narrative, the threat actors remedied many of the pitfalls that limited the NotPetya infections and thus the economic loss.

Table 8: Comparison of Bashe scenario losses to estimated NotPetya precedent

Scenario variants	Total economic loss estimates, $bn	Estimated NotPetya economic loss, $bn	Ratio of economic loss to NotPetya
S1	$85	$10.[46]	8
S2	$159		16
X1	$193		19

[46] PCS 2018

6. The growing cyber insurance market

6. The growing cyber insurance market

The first insurance products for cyber loss appeared in the 1980s and became a niche area of specialised insurance for liability from IT errors and omissions throughout the 1990s, boosted towards the end of the decade by fears of Y2K computer failures: the suspicion that date counters in computer software systems would not be able to cope with the date change from 1999 to 2000.

The 2000s saw the launch of innovative cyber insurance products to cover the third-party liabilities from data breaches, but initially these did not offer coverage for first-party losses and excluded anything resulting from rogue employees, and costs for fines, penalties, or regulatory actions. In the middle of the 2000s, coverage was added for first-party losses, for cyber business interruption, network asset damage, and cyber extortion. The US Health Insurance Portability and Accountability Act set new security standards for the protection of health information about individuals, together with regulatory penalties and reporting requirements for any data that was leaked. This spurred healthcare companies to take out cyber insurance and insurers to introduce special sub-limits for this coverage.

The growth of the cyber insurance market

In 2003 California became the first US state to pass a law requiring companies to notify state residents and regulators if personal information they held about them was accessed by an unauthorised person. The other US states have followed suit over subsequent years, each passing their own individual versions of similar laws, with additional Federal laws creating a patchwork regulatory framework for data protection. This wave of regulation sparked the formalisation of data protection management in US companies and drove the growth of demand for insurance to cover data-related liabilities. The initial market for cyber insurance was predominantly in the US.[47]

In the 2010s, due to both the increase of data exfiltration cyber-attacks and of regulations requiring them to be reported publicly, the number of data breaches hitting the headlines increased significantly. Publicly reported data breach events increased from just over 1,800 in 2009 to 6,700 in 2013.[48] Demand for cyber data breach insurance followed, with total premiums growing to over a billion dollars by 2015. The traditional cyber insurers were the main beneficiaries of this, but it also generated experimentation by specialist carriers offering insurance products for cyber property damage to energy companies, for example.

Premiums from affirmative cyber insurance products continued to grow rapidly to over $4 billion by 2017,[49] contrasting with nearly static premium growth from other lines of insurance during a 'soft market' for insurance products in general. As the cyber market expanded, it attracted other mainstream insurers to add cyber products to their lines of business. In 2015, fewer than 50 insurance companies were offering cyber insurance globally but, by 2018, more than 150 companies had affirmative cyber products available.

The market for cyber insurance has rapidly become international, driven by the geographical spread of cyber-attacks and business losses suffered by organisations in many countries, together with the accompanying proliferation of privacy protection regulation in many nations of the world. Data protection laws have been passed in 35 countries since 2010. The implementation of the General Data Protection Regulation (GDPR) across Europe in 2018 is credited with a resultant growth in demand for cyber insurance in many European countries.[50] Monitors of cyber insurance regulation identify over 70 countries that have passed data protection laws.

[47] Wells 2018

[48] Coburn, Leverett, and Woo 2019

[49] "Estimated Value of Cyber Insurance Premiums Written Worldwide from 2014 to 2020 (in Billion U.S. Dollars)" 2018

[50] Cohn 2018

Nearly all the major advanced economies are now under 'heavy' or 'robust' regulatory regimes for cyber loss, and emerging markets are increasingly regulated.[51] Although the majority of affirmative cyber insurance premium still comes from the US, there are now significant premiums being generated in another 30 countries, and the market is expected to be truly global in a few years.

Types of cyber insurance

Policies offered within the insurance industry can either be affirmative, meaning they explicitly cover cyber risk, or non-affirmative, meaning they are not explicit in their coverage. The following definitions are used when discussing these two types of policies.

- *Affirmative standalone cyber cover* – Specific standalone policies for data breach, liabilities, property damage, and other losses resulting from information technology failures, either accidental or malicious.
- *Affirmative cyber endorsements* – Cyber endorsements that extend the coverage of a traditional insurance product, such as commercial general liability.
- *Non-affirmative cyber exposure: gaps in explicit cyber exclusions* – There is a range of traditional policies, such as commercial property insurance, that have exclusion clauses for malicious cyber-attacks caused by nominated perils such as: Fire; Lightning; Explosion, and Aircraft Impact (FLEXA).
- *Non-affirmative cyber exposure: policies without cyber exclusions* – Many insurance lines of business incorporate 'All Risks' policies without explicit exclusions or endorsements for losses that might occur via cyber-attacks.

Data capture of a primary insurer's exposure to non-affirmative versus affirmative exposure still varies greatly. This creates a further challenge for reinsurers in accessing their exposure to non-affirmative cyber risks.

Characteristics of cyber risk

Corporate cyber insurance

Cyber insurance provides compensation for different elements of losses that companies could suffer. A CCRS study of coverage provided by affirmative cyber insurance products on the market identified 20 main types of cover, but with wide variation in products across the market.[52] These coverages can be triggered by a number of different cyber loss processes that can arise from malicious cyber-attacks and accidental malfunction of the information technology systems used by companies. Cyber losses can be broken down into several key processes or principal causes of how those losses arise. For example:

- *Data exfiltration* – the loss of confidential data from companies to unauthorised people that breach the privacy of their customers, employees, clients, or counterparties.
- *Contagious malware attacks* – malware that can spread and replicate through networks of communication and cause harm to the computer systems that it infects.
- *Denial of service attacks* – disruption to servers and website business activity by bombarding them with spurious traffic.
- *Financial transaction theft* – unauthorised transfer of funds through trusted transaction networks to syphon money away and not be recoverable.
- *Failures of counterparties or suppliers* – failures of third-party systems that companies rely on for their information technology services, such as software product providers, online service providers, cloud service providers, and others.

Although this is not an exhaustive list, these key loss processes are estimated to account for around 90% of the economic losses that business suffer as a result of cyber-attacks and technology failures.[53] Each of them is a distinctively different loss process with its own implications for cyber risk management and mitigation. To date, the greatest losses have arisen from data exfiltration, which is estimated to comprise around half of the losses suffered from cyber. This report provides a scenario for exploring in more detail the loss potential from contagious malware attacks.

Currently, most losses have been relatively routine or 'attritional'. The cyber insurance industry has not experienced a major systemic 'catastrophic' event that has triggered major claims from large numbers of policy holders from the same cyber-attack. In the period 2013 to 2018, the affirmative cyber insurance direct loss ratio across the industry has averaged around 50% – i.e. half of the premium was spent out in paying claims. This is a much higher margin and more profitable business than many other lines of insurance. Cyber insurance has attracted many new entrants as a result.

Many other longer-established classes of insurance business are characterised by multiple years of profitability, followed by a large event that triggers a very large loss for the whole industry resulting from large numbers of high cost claims, which wipes out many years of surplus.

[51] "DLA Piper Global Data Protection Laws of the World - World Map" n.d.

[52] Cambridge Centre for Risk Studies 2016

[53] A. W. Coburn et al. 2018

These catastrophe events form the tail risk for insurance lines, and many experienced insurance professions are concerned that the true catastrophe potential of cyber risk has not yet become apparent. Some commentators have suggested that this hidden potential for large future losses may make cyber uninsurable.[54] Others have warned of the dangers of writing cyber insurance without fully understanding the tail risk.[55]

Insurance companies have tended to be cautious when entering the cyber insurance market by offering low policy limits or writing endorsements on existing policies. These approaches have allowed insurers to build up multiple years' worth of claims experience and underwriting practice, thus improving their expertise in cyber as a risk. Some insurers, however, approach the market by offering large limits from the very start.

Insurers use hypothetical Probable Maximum Loss (PML) assessments of what extreme loss could be expected in the future. One of the greatest difficulties is assessing the annual probability (return periods) of large systemic losses that have never occurred in historical claims experience. Studies and scenarios like this one that explore the potential for future large scale systemic cyber loss catastrophes help the insurance industry improve their awareness of catastrophe risk and assist insurance companies in setting PML levels, assigning risk capital, and adding some level of catastrophe loading into the pricing of the insurance product to prepare for future shocks of large claim demands.

Counterfactual risk analysis, as explored in Lloyd's report '*Reimagining history*', would also provide insurers with the ability to search for and analyse data that may not be collected by historical real-world event research, and therefore could assist with the identification of unlikely but possible events.

Personal cyber insurance

The personal cyber insurance market has been growing over the years with the market getting more sophisticated. A Norton study found that 978 million adults in 20 countries have experienced a cyber-attack in 2017, costing an estimated $172 billion and taking 3 full business days to sort out.[56] Personal cybercrime is out pacing the more traditional crimes of burglary, robbery and car theft.[57]

Although, current products are targeted towards high net-worth individuals, there is a movement towards policies for all incomes. The following covers are now on offer for individuals:[58]

- *Identity theft expenses* – similar to data breach coverage for corporates, this coverage would compensate individuals when a data breach occurs. Further some insurers are offering risk mitigation support to help prevent such losses.
- *Online fraud* – this provides coverage for unauthorised online transactions
- *Extortion payments* – individuals are increasingly become targets of ransomware and thus need risk transfer solutions
- *Data restoration/recovery* – coverage for the recovery of data encrypt during a ransomware event
- *Social engineering* – this provides coverage for losses due to social media impersonations resulting in the transfer of money from relatives to the attackers
- *Cyber bullying* – this coverage provides support for assistance in responding to harmful statements or messages and even the undesirable spread of images[59]
- *Reputational harm* – individuals can suffer reputational damage especially in the case of social engineering and media related attacks
- *3rd Party Liability* – individuals may be held liable for events that impact others particularly when it comes to social engineering and media related liabilities

Experts believe that there will be a trend of offering cyber coverages as a part of property insurance in the next 10 years given the transition to smart homes and the integration of IoT devices. [60] It is estimated that an average household has 20 connected devices.[60] A study of US consumers found that 10% had suffered a cyber-attack on an IoT device in their home.[61]

Challenges for the development of the cyber insurance market

The 2019 global market of affirmative cyber insurance is estimated at $6.4 billion in premium, which is a sizeable industry but is a relatively minor line of insurance business. The total premium for the whole of the Property and Casualty insurance industry (non-life) is over $2 trillion. Projections for future growth of the cyber

[54] "Is Cyber Risk Uninsurable? Its 50/50 Says PwC" 2016

[55] Kim 2018 reports Warren Buffett's warning that '*Cybersecurity risk is uncharted territory*'

[56] Norton by Symantec 2018

[57] Delta Insurance 2018

[58] OECD 2017

[59] Claire 2016

[60] Ralph 2017b

[61] OECD 2017

insurance market range from the aggressive to the stratospheric. Some commentators see cyber insurance moving from a niche specialised line of insurance to being a standard peril covered in all lines of insurance, as commercial purchasers of insurance need to protect their digital assets in the same way that they once needed to protect their physical assets of production.

The reality, however, is that commercial companies need to obtain significant protection from purchasing cyber insurance far beyond what the market is currently making available. Insurers are understandably being cautious by offering low limits to protect their own loss potential, but this strategy may fail to meet commercial needs for protection and may make insurance a less attractive option for cyber risk management. An estimated half of all global cyber insurance policies sold are for limits of less than $1 million. Limits of over $10 million are becoming more common (although currently estimated as less than 10% of policies written globally) and for a company to obtain cyber insurance coverage of $100 to $500 million requires the construction of complex towers of coverage involving many different insurance companies each taking small slices. Limits are increasing over time as insurers gain confidence, but these might still lower than the amount of cyber insurance cover that is being requested by the market. Companies face cyber losses that could potentially amount to many hundreds of millions of dollars. It is estimated that the insurers bear less than 10% of the cyber losses that occur each year.[62]

Companies in total are spending around $6 billion a year in buying cyber insurance[63], which contrasts with expenditure of over $120 billion annually on cyber security.[64] It is logical that spending on loss prevention (security) would be higher priority than buying loss compensation (insurance), but in other areas of corporate risk, such as fire protection in factories, the two areas of expenditure (loss control through fire prevention engineering and fire insurance purchasing) are more evenly balanced.

Analysts suggest that, over time, insurance should grow to become a larger share of the amount that organisations spend on cyber risk management. However, if companies cannot protect against more than 10% of their potential future losses, because they can only obtain policies with small limits, then insurance will stay as a limited component of their risk management strategy. For cyber insurance to become a significant sized market, companies need to be offered limits that are meaningful against the losses that they face. For insurance companies to offer larger limits, they must increase the capacity that they make available to cyber. Capacity allocation depends on insurance companies feeling confident that they have adequately assessed, and priced in, the risk of cyber catastrophe.

Studies like this one are intended to help insurers assess cyber tail risk more realistically and to allocate capacity to offering their policy-holders realistic premiums for the coverage and capacity that will give them the protection they need.

Enabling a strong growth market for cyber insurance in Asia

Asia is one of the fastest-growing markets for cyber insurance with established cyber insurers now offering products in across the area. Market analysts saw an overall 87% increase in cyber insurance take-up rates in Asia in 2017 with the current premiums estimated to be $50 million.[65] It is estimated that 1 to 20% of companies in Asia are insured against data breaches, with premiums expected to increase to $500 million to $1 billion by 2025.[66] Further, it is estimated that only 8% of Asian companies are insured against contagious malware events. Given the increase in cyber-attacks in 2017 in the Asian market, companies are now more likely to have standalone cyber insurance with business interruption cover.

The Asia-Pacific Economic Cooperation (APEC) developed a Privacy Framework along with a Cross-Border Privacy Rules scheme (APEC CBPRs) that has been adopted by several countries in the alliance. Some countries have gone above and beyond this initial framework to create bespoke data privacy regulation and several established regulations seem to be under constant revisions. This creates a complex regulatory landscape in Asia.

Further developments include the ASEAN-Singapore Cyber Center, which will support members states' cyber strategy development, legislation, and research capabilities and provide virtual cyber defence training, and the CyRiM project, which aims to create an efficient cyber insurance market.[67]

Data privacy regulation is a catalyst for further cyber insurance uptake. For multi-national corporates based in Asia with operations in Europe, we are also likely to see the new GDPR regulation in Europe drive insurance take-up as well.

[62] A. Coburn, Leverett, and Woo 2019

[63] PwC 2018

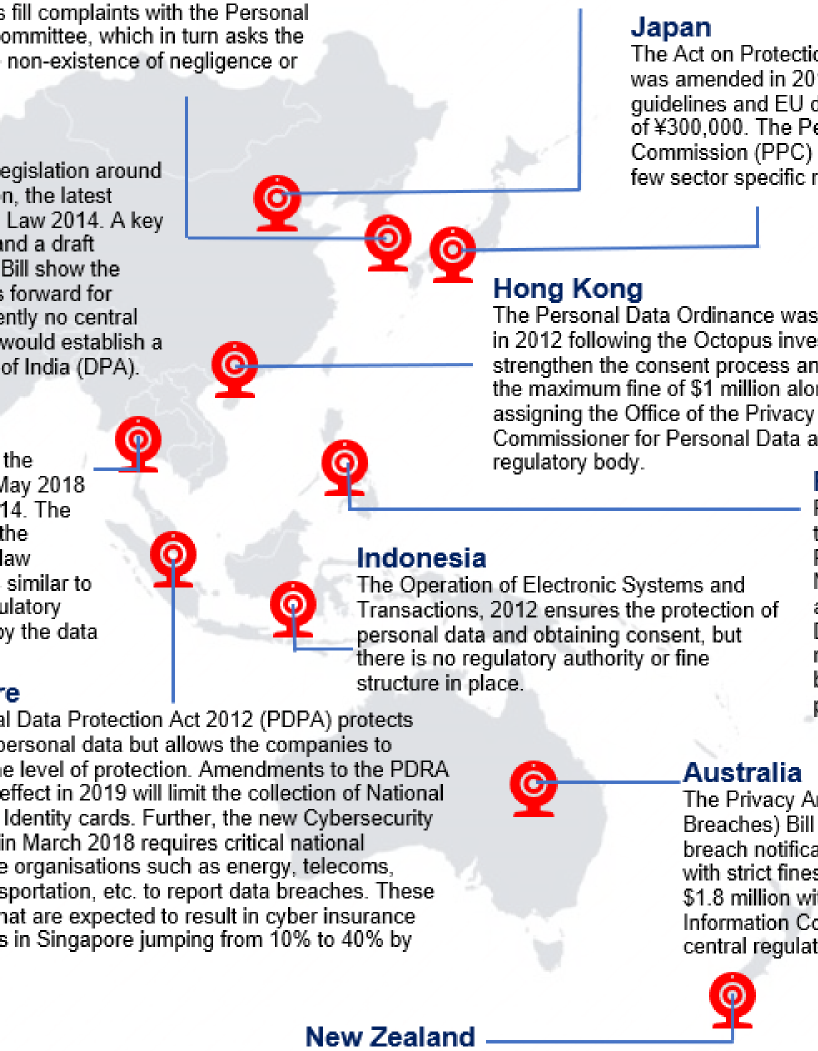
[64] Morgan 2017

[65] Williams 2016; Weinland 2017; OECD 2017

[66] JLT 2018; OECD 2017

[67] CNA n.d.; NTU-IRFRC n.d.

Figure 5: Data protection laws in the Asia-Pacific region[68]



Republic of Korea

Revisions to the Act on Promotion of Information and Communications Network Utilization and Information Protection will come into effect in June 2019 and requires information communication providers to take out insurance or hold significant cash reserves in case of a data breach, also imposing up to $20,000 fines. Korea has an interesting model for loss resolution in that consumers fill complaints with the Personal Information Dispute Mediation Committee, which in turn asks the defendant company to prove the non-existence of negligence or infringement.

China

The Personal Information Security Specification came into effect in May 2018 and lays the groundwork for data protection in China. Still not clear on who the regulatory authority is for data protection; there are some sector specific ones.

Japan

The Act on Protection of Personal Information (APPI) was amended in 2017 and is based on OECD guidelines and EU directives. It sets a maximum fine of ¥300,000. The Personal Information Protection Commission (PPC) acts as the main regulator with a few sector specific regulators involved.

India

India has a patchwork of legislation around data privacy and protection, the latest being the Right to Privacy Law 2014. A key Supreme Court decision and a draft Personal Data Protection Bill show the potential for positive steps forward for consumers. There is currently no central regulator but the draft bill would establish a Data Protection Authority of India (DPA).

Hong Kong

The Personal Data Ordinance was updated in 2012 following the Octopus investigation to strengthen the consent process and increase the maximum fine of $1 million along with assigning the Office of the Privacy Commissioner for Personal Data as the lead regulatory body.

Thailand

The Thai cabinet have approved the Personal Data Protection Bill in May 2018 that was initially introduced in 2014. The bill is now undergoing review by the Council of State. If enacted, this law features several data protections similar to GDPR. There is no standard regulatory body, but fines can be imposed by the data controller.

Philippines

Privacy is explicity protected in the constitution and the Data Privacy Act of 2012. The National Privacy Commission acts as a regulatory body. The Data Privacy Act of 2012 set a maximum penalty at $100,000 but included imprisonment provisions.

Indonesia

The Operation of Electronic Systems and Transactions, 2012 ensures the protection of personal data and obtaining consent, but there is no regulatory authority or fine structure in place.

Singapore

The Personal Data Protection Act 2012 (PDPA) protects consumers personal data but allows the companies to determine the level of protection. Amendments to the PDRA coming into effect in 2019 will limit the collection of National Registration Identity cards. Further, the new Cybersecurity Bill enacted in March 2018 requires critical national infrastructure organisations such as energy, telecoms, utilities, transportation, etc. to report data breaches. These are drivers that are expected to result in cyber insurance take-up rates in Singapore jumping from 10% to 40% by 2020.

Australia

The Privacy Amendment (Notifiable Data Breaches) Bill 2017 requiring mandatory data breach notification started in February 2018 with strict fines ranging from $360,000 to $1.8 million with the Office of the Australian Information Commissioner (OAIC) as the central regulatory body.

New Zealand

A new Privacy Bill was proposed in March 2018 to replace the 25-year-old Privacy Act. Although requiring an update, the Privacy Act of 1993 was advanced for its time, regulating how companies use, disclose, and retain personal data. The new bill would require mandatory data breach reporting with fines up to $10,000 and the ability of the commissioner to issue compliance notices.

[68] Sacks 2018; Balaji n.d.; UNCTAD 2016; Trilegal n.d.; UNCTAD 2016; Boonklomjit et al. 2018; Privacy International n.d.; Huang n.d.; Kwang 2017; “Reforms to Singapore Personal Data Protection Law in Force from 2019” 2018; Cramer et al. 2018; Williams 2016; Weinland 2017; Wall n.d.; The Law Reviews 2017; Office of the Australian Information Commissioner (OAIC) n.d.; Marshall 2017; Hedrich, Wong, and Yeo 2017; DLAPiper 2017; Reidy 2018

7. Insurance industry loss estimation

7. Insurance industry loss estimation

The CCRS insurance industry loss estimation for the 'Bashe attack: Global infection by contagious malware' scenario considers cyber exposure from affirmative and non-affirmative cyber cover. The loss estimates derived from this model reflect the likely pay-outs for the global insurance market in 2019. The 2019 structure is the result of projections from the 2018 insurance penetration and incorporates rates of regional growth in insurance penetration, limit and deductibles structure, and gross written premiums based on an extensive literature review and analysis of current growth trends in the cyber insurance market.

In this scenario, attackers are not engaging in terrorism or warfare so the Terrorism Risk Insurance Act (TRIA) in the US would not be triggered. The totals for insured losses around the globe resulting from the Bashe scenario are shown in Table 9 below. This table outlines the insured losses by type of claimant, coverage, and the scenario variant. Close examination of these results indicates that Business Interruption (BI) coverage is the main driver of loss, which encompasses 71% of total losses for S1 followed by incident response costs, and Liability. BI in this report applies to revenue.

Table 9: Estimated global insured industry losses by scenario variant, $ billion[69]

Claimant type	Coverage	S1	S2	X1
Companies directly impacted	Business interruption (Affirmative cyber)	$4.8	$6.4	$10.7
	Business interruption (Non-affirmative cyber)	$2.4	$3.2	$5.3
	Cyber extortion	$0.2	$0.2	$0.4
	Incident response costs	$1.4	$1.9	$3.1
	Liability	$0.8	$1.5	$2.5
	Data and software loss	$-	$-	$2.5
Companies indirectly impacted	Contingent business interruption	$0.2	$0.2	$0.3
	Liability	$0.3	$0.8	$1.2
Defendant companies	Liability (technology errors & omissions)	$0.1	$0.3	$1.3
Grand total insurance, $bn		$10.2	$14.5	$27.3

[69] These losses consider insurance penetration, policy limits, and deductibles.

It is important to note that 'data and software loss' is only present in the X1 scenario due to the change in payload for the malware. In the narrative for the X1 variant, the payload is a back-up wiper that deletes the infected network and backup files for companies. This loss is not present in the narrative of S1 or S2. The appendix provides a guide on how to calculate the insured loss for a company-specific portfolio for the Bashe scenario.

We stress that the assumptions in general and in particular for Liability are highly speculative. This is only one possible scenario and the split of losses between classes or steepness of trend between scenarios could be higher or lower depending on specifics of any real event and the decisions of the courts.

General model assumptions

To estimate the total insurance industry losses, CCRS assumes a policy limit and deductible structure based on a distribution around average limit values by company size. Limits are assumed to range from $500,000 to $200 million and a distribution is applied to this range based on suggested average limits in the market.[70] For example, it is assumed that 70% of premier companies have a policy limit equal to or greater than $100 million while for small companies it is assumed that 50% have a policy limit equal to or less than $5 million. Policy deductibles are assumed to be 5% of the limit. Exposures are determined at a coverage level and summed for comparison to the policy limit and deductibles.

Reports in 2016 suggested that the US made up 90% of written premium with Europe at 4% and the rest of the world at 6%.[71] Based on the growth of cyber insurance uptake in the European and Asian markets, CCRS assumes the following country-level insurance distribution shown in Table 10 for 2019. This country-level distribution is further distributed by company size. For example, we believe that 28% of large companies in the US have cyber insurance, this is in line with an OECD report suggesting 20 to 35%.[72]

Table 10: 2019 Regional cyber insurance distribution by country[73]

Region	Regional Cyber Insurance Distribution
United States	70%
Europe	20%
Asia	8%
Rest of World	2%

Using the penetration rates above and taking the number of infected companies from the economic modelling, the number of companies that are infected, have insurance, and notify their insurers of a loss can be estimated at 9%.

Table 11: Number of companies with cyber insurance that are infected

	S1	S2	X1
Number of infected companies from economic modelling	250,000	501,000	613,000
Number of infected companies that notify insurers of a loss and have insurance	21,000	43,000	53,000
% of infected companies that notify insurers of a loss and have insurance	9%	9%	9%

[70] Sub-limits are not taken into account in this modelling

[71] Hedrich, Wong, and Yeo 2017

[72] OECD 2017

[73] CCRS assumption

Claimant types

The loss from this scenario derives from the following claimant types:

1. Companies directly impacted by the malware attack. Companies that are infected by the ransomware see resulting losses due to IT failure and unavailability of data for the continuation of business. These companies suffer significant business interruption due to the encryption of data used by information technology (IT), operational technology (OT) and connected systems, incident response costs, data and software loss costs in response to the ransomware incident, and costs associated with cyber extortion. There may also likely be claims made against directors and officers who failed to act in the best interest of their company resulting in a share price drop and litigation from shareholders. Litigation costs and settlements are claimed under the defendants' Directors and Officers (D&O) coverage.

2. Companies indirectly impacted by the malware attack. A category of companies that are not infected by the ransomware but are negatively impacted through third-party IT and vital supply chain failures. These companies will claim against the contingent business interruption in their cyber affirmative insurance. They could also see some claims against directors and officers should they suffer a share price drop due to the contingent business interruption.

3. Defendant Companies. Third-party IT service companies sued by firms directly and indirectly impacted by the ransomware. Defendant companies are likely to be different information technology firms that failed to provide adequate technical services including: custom application developers digital service companies such as cloud operation e-commerce/financial systems platform, data hosting, and network content delivery providers that fail due to the ransomware, and other firms and service involved with the vector of introducing malware into companies. Litigation costs and settlements are claimed under the defendants' Technology Errors and Omissions (TechE&O) coverage in their cyber affirmative insurance policies**.**

Companies directly impacted

Business interruption

Affirmative cyber BI

The infection of IT, OT, and smart devices prevents companies from selling goods and services, disrupts their internal management, limits their ability to make payments to suppliers, and hampers their communications. Companies incur significant costs as productivity, sales, and general business activities are impacted for the duration that systems remain infected. The failure of the IT systems and networks triggers claims under business interruption coverages from firms' cyber affirmative policy. The insured loss is calculated by applying the limits and deductibles structure as outlined in the 'General Model Assumptions' section to the average direct BI economic loss per company for the duration of discontinuation of business activities. CCRS has assumed a lower bound of 24 hours and an upper bound of 30 days as the period of business interruption that costs can be claimed. This max business interruption period was derived from studying historical precedents of ransomware event recovery period. The drivers of loss result in the variance of direct losses across sector and size of companies. Companies with a longer business interruption duration, which results in higher BI claims, holding size constant, are within sectors that have a higher Sector Vulnerability Score and Sector Criticality Score.

Non-affirmative cyber BI

There could also be exposure in the traditional property books under BI. Following the significant business interruption from the NotPetya cyber-attack, Maersk (a global shipping company) has reportedly attempted to claim the BI losses under their traditional property related BI policies. Due to the extent of damage to their IT systems, Maersk had to replace 4,000 servers and 45,000 PCs all while rebuilding 2,500 apps - this was estimated to cost Maersk up to $300 million. [74] Further, Merck (a global pharmaceutical company) has one of the largest reported cyber affirmative claims at $275 million with a potential non-affirmative exposure of $640 million on their traditional property tower, although no claims have been reported to date.[75] The NotPetya attack is estimated to have an economic cost of $10 billion. Surprisingly, $3 billion of this loss was covered by affirmative cyber coverage and non-affirmative traditional property coverage.[76] CCRS has assumed a lower bound of 24 hours and an upper bound of 30 days as the period of business interruption that costs can be claimed.

[74] Chirgwin 2018

[75] Reinsurance 2018

[76] "PCS: NotPetya Insured Losses Now $3bn+" n.d.

Box 8: Litigation surrounding damage to IT assets

Several US lawsuits have debated this topic of whether damage to IT assets and data constitutes physical damage and thus coverage under a traditional property policy. The following list has been adapted from several sources on notable IT physical damage litigation: [77]

- *Am. Guarantee v. Ingram, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. 2000)* – found that physical damage was not limited to destruction but "lack of access, loss of use, and loss of functionality".
- *Lambrecht v. State Farm Lloyds, 119 S.W.3d 16 (Tex. App. 2003)* – found that hard drives that could no longer store information were physically damaged. The appellate court reversed this judgement in favour of the insurer.
- *NMS Services, Inc. v. The Hartford, 62 Fed. Appx. 511 (4th Cir. 2003)* – found the insurer responsible for paying a claim for business interruption from a traditional property policy following an attack by a disgruntled employee.
- *Ward General Insurance Services Inc. v. Employers Fire Insurance Company, 7 Cal.Rptr. 3d 844 (Cal. Ct. App. 2003)* – found in favour of the insurer, arguing that an operator mistake causing the crash of a database was not physical damage
- *Southeast Mental Health Center Inc. v. Pacific Ins. Co. Ltd., 439 F. Supp. 2d 831 (W.D. Tenn. 2006)* – found that the loss of computer systems during severe weather was covered under a traditional BI policy.

Box 9: Ambiguity in cyber business interruption coverage

The WannaCry and NotPetya cyber events in 2017 highlighted the growing need for cyber business interruption coverage, as large major corporations like Maersk, FedEx, Deutsche Bahn, and Renault saw several-day disruptions of critical internal IT systems.[78] Not all cyber BI policies are alike in the type of events they cover. Some policies cover all three of the following event triggers while others cover only one.[79]

1. *Malicious threat actor* – business interruption cover where the threat actor has malicious motivations, such as the intent to cause harm or property damage to the target. Malicious motivations are typically associated with cyber criminals or nation-state threat actors. For this Contagious Malware scenario, it is key that insureds have wording for malicious threat actors to receive a claim award.

2. *Unplanned system outage due to negligence* – in this case business interruption cover could result from an accident by an employee that causes the disruption.

3. *Unplanned IT supply chain disruption* – business interruption cover resulting from an unplanned event at an external IT service provider. This BI coverage potentially overlaps with CBI coverage. Further, so insurers are offering the IT service provider failure as system failure coverage. As not all insurers have adapted this IT supply chain disruption into their BI coverages, we choose to model this loss separately as CBI.

Further, it is important to review any exclusions on cyber BI policies that may limit cover. "Many insurers have "failure to patch" exclusions, which exclude any and all coverage for any and all damages in the event that the vulnerability had been previously identified and not patched."[80]

[77] Clyde&Co 2018; Miller 2018

[78] Ghosh 2017

[79] Buck 2018; JLT 2018a

[80] Aon Risk Solutions, n.d.

Cyber extortion

For each device infected within a company, the ransomware encrypts all files and demands a ransom to be paid in cryptocurrency to decrypt the data. The incident generates cost through the payment of the ransom, potential expenses charged by professionals to negotiate with the cyber criminals, and the cost of hiring outside security experts to prevent future extortion attempts. Cyber extortion will similarly be claimed under cyber affirmative policies.

It is important to note that while in this scenario the files are decrypted when victims pay the ransom, this is not often the case. Paying a ransom does not reliably result the decryption of files.**[81]** Companies could also suffer reputational loss if their ransom payments are disclosed to the public.

Incident response costs

The incident will generate further costs for companies directly impacted due to necessity for emergency response, forensic investigation into the scale and scope of the infection, the subsequent clean-up of systems, post-event investigation, and minimisation of post-incident losses. The technical response will include patching the vulnerability and investigating the attack vector used by the threat actors to prevent a reoccurrence, removing the malware, decrypting infected systems, and reinstating the data files in S1 and S2 from the backups. Incident response costs will be claimed under affirmative cyber policies. The costs of upgrading compromised systems is often not included in incident response coverage so cannot be claimed by the victims. The incident response cost will derive from both internal staffing costs and external cyber security consultants hired to work on-site until the company is back online.

This coverage does not include any public relation or reputational damage costs.

Liability

Lawsuits may be filed due to the failure to prevent, and any mishandling of, the cyber-attack, causing a share price drop and a potential violation of the directors' and officers' fiduciary duty owed to shareholders. Companies that suffer a greater infection rate and duration of interruption are likely to perform worse than their nearest competitors, resulting in a greater relative negative shock on stock price valuations. This in turn increases the likelihood of legal actions against executives of a company by their shareholders.

Taking account of the small number of companies expected to be affected and the lawsuits arising, we estimated the likely costs as shown in Table 9. The exact quantum of these losses is uncertain as is the number of lawsuits or indeed, the frequency of success. The figures in Table 9 should therefore be taken as speculative.

D&O insurance penetration is highest in the US market, with Germany and Australia experiencing recent growth in litigation.[82] Thus, most of the losses will be focused on the US market.

Box 10: Directors and Officers litigation

In the past years, D&O litigations brought against Target, Wendy's, Home Depot, and Wyndham by customers for failing to prevent data breaches and by shareholders for breach of fiduciary duty have all been dismissed successfully.[83] However, lawsuits continue to be filed with similar arguments, with Equifax being the most recent. Yahoo even settled their shareholder class action lawsuit for $80 million in early 2018.[84] The SEC has issued guidance on reporting cyber security concerns.[85] An Aon Stroz Friedberg 2018 report found that cyber rank third in shareholder D&O litigation and is expected to increase this year.[86] This is a growing area of litigation that could potentially add to an insurer's accumulation risk.

Data and software loss (X1 only)

In the X1 variant of the scenario, the ransomware is combined with a *back-up wiper* that permanently deletes all back-up files from the infected system. Companies infected by this wiper will attempt to recover this data using in-house and external expertise. This process will involve attempts to recover data from cloud infrastructure, shared network files that are not encrypted, email, or even external storage devices that range from outsourced data centres to USB sticks. While some data can be recovered, most data is lost permanently.

Data and software loss costs will be claimed under cyber insurance policies. The cost of decrypting data is not included in data and software loss coverage as the data must be activity deleted or corrupted so that a 'reconstitution of data' can occur.

[81] Chris Baraniuk 2017

[82] Barlow 2016; Clyde&Co 2018b

[83] DAC Beachcroft 2017

[84] Turpin and Meagher 2018

[85] SEC.gov 2018

[86] Hook 2018

Companies indirectly impacted

Contingent business interruption

The impact of the ransomware scenario causes contagion effects that results in companies being indirectly impacted through their supply chains (both physical and digital). The infection of digital services due to the cyberattack results in both upstream and downstream supply chain shocks due to failure of goods being delivered (both intermediary and final), disruption in services and point-of-sale activities that are vital to the continuation of business.

Cyber contingent business interruption (CBI) coverage covers the insured's loss of income and operating expenses due to the disruption of 3rd party digital services and supply chain interruptions.[87] The insured loss is calculated by applying limits and deductibles outlined in the General Model Assumptions section above to the average indirect economic loss for the duration of the contingent business interruption and is claimed under a cyber affirmative policy. It is likely that the supply chain shock will result in insured losses from Cyber CBI insured loss was expected to be significantly greater than estimated due to the high indirect economic loss. However, the penetration of CBI coverage is comparatively low, resulting in a 'protection gap'.

Liability

As with companies directly impacted by the cyber-attack, firms indirectly affected may see the same cyber liability policies come into effect. The directors and officers of the companies indirectly impacted by the scenario also have the same legal responsibility as firms directly impacted to prepare and action contingency plans should a cyber-attack occur. Negligence from directors and officers may result in the contagion impact on their supply chain indirectly affecting their company more severely than others, resulting in a greater share price devaluation.

Defendant companies

Technology Errors and Omissions

CCRS assumes that a limited number of companies directly impacted by the ransomware attack sue their IT service providers, who fail to provide IT services due to outages in their systems, and whom companies deem as culpable in not protecting their systems from malware vulnerability. The plaintiffs claim the net losses they suffer that they have not been able to recover from their insurers including: losses above limits, non-insured losses, and co-insurance deductibles.

Defendant companies could include:

1. Digital services companies including: cloud operation e-commerce/financial systems platform, network content delivery providers, email hosting services and data hosting and processing services
2. Custom application development services that are involved in the transmission of the malware
3. Other firms involved with the vector introducing malware into companies

IT companies that inadequately provide their third-party digital services due to the infection of systems resulting from the cyber-attack may receive claims from the companies directly impacted by the digital service provider outage. Companies that provide other services involved in the vector of attack may be subjected to litigation as well.

Liability loss assumptions

CCRS assume that defendant companies carry liability insurance and that the claims triggered are from coverages including but not limited to technology errors and omissions (Tech E&O). These companies take control of litigation as soon as notification of the suit occurs. Investigating the chain of liability is complex due to the global scope and complexity of the cyber-attack, which leads to a prolonged investigation into identifying the vulnerabilities, defects and actions leading to infection. CCRS assume that there are only 3 Tech E&O-related lawsuits in S1, 6 in S2, and 30 in X1. The defendants expected loss is $3 million. We have assumed a low incident rate and loss amount as this is a new and emerging area of litigation.

Box 11: IT vendor liability

A malware event at [24]7.ai impacted Delta Airlines in Fall 2017 resulting in a data breach concerning personal and credit card information transmitted on the Delta website using an online chat service provided by [24]7.ai.[88]

A lawsuit filed by customers impacted by the data breach names both Delta and [24]7.ai with Delta continuing to place 100% of the liability on [24]7.ai.[89]

[87] OECD 2017

[88] Delta 2018

[89] Yamanouchi n.d.

Additional areas of insured loss not included in estimate

This scenario could result in claims from other classes of business outside of cyber as well as additional coverages within the cyber class of business that were not modelled. For example:

Public relation expenses

Companies that are heavily impacted by the malware event may need to support to deal with the negative media attention they receive. This is a unique cover that some insurers are offering to support the costs of engaging a public relations firm, which is not typically a part of other cyber coverages.[90] Sometimes this is coupled with a crisis management cover.[91]

Reputational damage

Again, for companies that are most impacted by the scenario they may see customer churn or reduced transaction volumes which can be directly attributed to the malware event and its effects on their operations. Reputational damage cover will support losses in revenues due to consumer shifts following the event. Further, there is a small but growing market for personal reputation cover that supports reputational damage losses for individual directors.[92]

Professional Indemnity/Liability

There is potential for professional indemnity claims for breach of contract should a firm not be able to provide services to their clients following the malware incident. DLA Piper, one the largest law firms globally, saw significant disruption following the NotPetya malware attack in June 2017 with a full day without phone service, six days without emails and another two weeks without access to old emails.[93] This interruption of IT services internally limited their ability to provide services to clients externally and in some cases caused them to not fulfil contracts. Breach of contract is a less common coverage on professional liability policies.

There is further potential for a breach of confidentiality claim on professional indemnity policies when data is exfiltrated, as in the X1 scenario variant.

Network security failure liabilities (3rd party liability)

This is third party liability coverage for cases where the malware is transmitted from one party to another with the primary party being held liable for third party damages.[94] There is likely to be 3rd party losses in this scenario as the malware is covertly forwarded to the victim's entire address book which can include external organisations and people.

IoT device bricking

Companies whose IoT or smart devices that are rendered useless follow the malware infections as ransoms were not paid to unlock them, could file a claim or replacement of the computers. Following NotPetya and WannaCry claims were made to this extent against Commercial General Liability (CGL), TechE&O and Cyber BI and Traditional BI policies.[95] There is much debate as to what type of insurance should cover this loss and thus some insurers are starting to offer bricking cover as part of a Cyber BI policy.[96]

Kidnap & Ransom (K&R)

Following the WannaCry cyber-attack in 2017 insurers saw an increase in claims against K&R policies with insureds arguing that the ransom payments and crisis management losses should be covered under these non-cyber policies as they are similar in nature to kidnap extortion events.[97] This is an area to watch as insurers may tighten up policy wording to limit their K&R exposure to cyber ransomware events or continue to leave non-affirmative exposures in their K&R responsibilities.

Product Liability

Similar to Tech E&O liability claims for faulty IT related services, product liability claims focus on software or hardware that enabled the malware to execute or spread due to unknown vulnerabilities. Litigation may arise from firewall and malware systems that fail during the cyber-attack. There is a school of legal thought that states that under the strict liability legal doctrine, individuals who suffered harm or property damage due to product defects have a potential valid argument even if the defect was previously unknown to the software manufacturer. "Therefore, strict products liability cannot be transferred from product to user via contract, which renders infeasible the common practice in the software industry of absolving liability for the vendor through End User Licensing Agreements."[98] This is an emerging area of litigation as the technology is advancing faster than the legal doctrine thus creating the potential for losses related to this Contagious Malware scenario.

Personal cyber losses

As the ransomware is forwarded to victims' entire contact list, there is potential for impacts to personal computers. Claims will likely be seen for personal cyber extortion payments as well as data restoration in the X1 scenario variant. Finally, there is potential for personal reputational policies to payout following the event.

[90] Twersky 2015

[91] OECD 2017

[92] Delta Insurance 2018

[93] Crowe 2017; Thompson 2017

[94] OECD 2017; Cambridge Centre for Risk Studies 2016

[95] Reuhs 2016; Trice 2018

[96] Lenihan 2018

[97] Barlyn and Cohn 2017

[98] Dean 2018

The results in context

The estimated global insurance industry loss is $10.16bn to $27.27bn for this Bashe scenario. A comparison of the losses to the economic loss and to the 2019 estimated cyber insurance premium helps put these losses in context. Comparing the insurance loss estimates to the economic losses shows that the insurance industry losses stayed within 9 to 14% of the economic loss. The estimated 2019 cyber affirmative insurance premium is $6.4bn,[99] which puts the affirmative cyber insurance industry loss estimates at 1.2 to 3.4 times the annual affirmative cyber insurance premiums.

Table 12: Bashe scenario global insurance industry loss estimates in comparison to global economic loss

Scenario variant	% of infected companies that notify insurers of a loss and have insurance	Total economic losses, $bn	Total o insurance industry loss estimates, $bn	Ratio of losses estimated as likely to be paid out under cyber affirmative coverage to total annual global cyber affirmative premiums[100]	Insurance loss as a % of economic loss
S1	9%	$85	$10	1.2	12%
S2	9%	$159	$14	1.8	9%
X1	9%	$193	$27	3.4	14%

Comparisons of the Bashe scenario estimated insured losses show that they range from 2 to 9 times the estimated insured losses from the NotPetya attacks in 2017, shown in Table 13. Further, the estimated economic loss for the NotPetya attack is $10 billion, which puts the insurance loss at 30% of the economic loss. This is an interesting comparison as it highlights the increased exposure of the insurance industry to these contagious malware attacks.

Table 13: Bashe scenario global insurance industry loss estimates in comparison with estimated historical precedent

Scenario variants	Total insurance industry loss estimates, $bn	Estimated NotPetya insured loss, $bn	Ratio of insured loss to NotPetya
S1	$10	$3.[101]	3
S2	$14		4
X1	$27		9

[99] This is calculated by interpolating between the 2015 and 2020 projections summarised in a Financial Times article by Ralph 2018.

[100] This is calculated by summing all the losses minus the non-affirmative BI losses and dividing by the estimated 2019 insurance premium.

[101] PCS 2018

8. Conclusions

8. Conclusions

This report deepens insurers' and risk managers' understanding of cyber-risk liability and aggregation. It shows the vital contribution research and analysis can make in reducing uncertainty concerning cyber risk.

The scenario highlights the extent of the damage that can occur from ransomware attacks and challenges assumptions about cyber preparedness. It also helps companies benchmark their risk management procedures.

The cost to the global economy

The scenario in the report shows the economic damage to the world economy from a concerted global cyber-attack, spread by a malicious email, may range from $85 billion (in the least severe scenario, S1) to $193 billion (in the most severe scenario, X1). The total amount of claims paid by the insurance industry is estimated to be between $10 billion in S1 and $27 billion in X1 (where the loss of data from the malware triggers additional claims for data and software loss).

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.

Analysis of these results shows that Business Interruption coverage is the main driver of the insured losses (71% of total losses for S1 and 59% for X1).

Drivers of losses

In the scenario and its variants, one of the main drivers of the direct and indirect global economic losses is the number of premier companies infected because they have the highest potential for total revenue loss. With premier companies modelled as having more than 1,500 times the daily revenue of small companies, their higher relative rates of infection make up a significant part of total global economic losses. In addition to greater business interruption and revenue losses, the increase in the number of infected devices increases the clean-up and cyber extortion costs.

Regional disparities in the economic loss estimates are caused by several financial and technical drivers. One of these is the diversity of business activity across regions. The sectoral breakdown of economic activity per region significantly influences the level of economic loss. As discussed in Section 3, some sectors are more vulnerable to both external and internal malware infection than others. Research into the resilience of companies to ransomware attacks found that those in the service sectors such as retail, finance, and tourism and hospitality, tend to be more vulnerable than those in the industrial sector (manufacturing being the exception). This may be due to their reliance on e-commerce as a significant revenue stream. These findings were built into the model, meaning regional economies that are more service dominated, such as the US and Europe, suffer greater relative infection and thus higher direct losses.

The penetration of connected systems per sector also affects the regional impact of the cyber-attack in the scenario. Sectors that have more connected systems, particularly those that are critical to business continuity, are more likely to suffer more severe and longer-lasting impacts on revenue. This particularly impacts regions where the output of the economy is dependent on manufacturing, healthcare, mining and other primary industries.

The distribution of company size across regional economies also influences the scale of the losses. Premier-sized companies contribute significantly to economic losses in the scenario, so regions with a higher number of premier-sized companies are more likely to experience higher losses.

Other drivers of differences in economic losses between regions include: commercial device and internet penetration per region, share of global Internet of Things (IoT) devices, and the number of third-party providers of IT services and products. These all determine the number of points that can be attacked, which in turn determines the contagiousness of the ransomware attack.

Insurance impacts

A comparison of the insurance losses to 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 the extent of underinsurance should such an attack take place.

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. [102] This shows the insurance industry is significantly exposed to a contagious malware event.

Lessons learned

This scenario emphasises to organisations – individual entities, industry associations, markets and policy makers – the importance of raising awareness of the risk, assessing the potential damage it could cause, and integrating effective responses within their business-as-usual practices.

There are lessons for the insurance sector, too, 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.

Insurance opportunities

There are also opportunities for insurers to grow their business in the classes associated with ransomware attacks. For example, Asia is one of the fastest-growing markets for cyber insurance with established cyber insurers, now offering products in across the area.
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.[103] Given the increase in cyber-attacks in 2017 in Asia over recent years, companies in the region are more likely to have standalone cyber insurance. Further insurance take-up is likely in the future.

The US is the world's most developed cyber market but 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' in this report help insurers expand their view of cyber risks ahead of the next event and help them, create new products and services that can make businesses and communities more resilient.

Future research

'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, Singapore 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.
The second report by this initiative will explore the impact of a cyber-attack on multiple port management systems.

[102] 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.

[103] Williams 2016; Weinland 2017; OECD 2017

References

Aon Risk Solutions. n.d. “Client Alert: WannaCry Cyber Attack.” http://www.aon.com/attachments/risk-services/cyber/Client-Alert-WannaCry-Cyber-Attack.pdf.

Ashford, Warwick. 2018. “Cyber Threat to Industrial Control Systems Highest Yet.” Computer Weekly. March 2, 2018. https://www.computerweekly.com/news/252436129/Cyber-threat-to-industrial-control-systems-highest-yet.

Balaji, Sindhuja. n.d. “India Finally Has A Data Privacy Framework -- What Does It Mean For Its Billion-Dollar Tech Industry?” Forbes. Accessed September 11, 2018. https://www.forbes.com/sites/sindhujabalaji/2018/08/03/india-finally-has-a-data-privacy-framework-what-does-it-mean-for-its-billion-dollar-tech-industry/.

Barlow, Noona. 2016. “Rise of the European Shareholder Class Action?” Claims Intelligence Series. AIG. https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/aig-claims-class-action-white-paper-final.pdf.

Barlyn, Suzanne. 2017. “Global Cyber Attack Could Spur $53 Billion in Losses: Lloyd’s of London.” Reuters. https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB.

Barlyn, Suzanne, and Carolyn Cohn. 2017. “Companies Use Kidnap Insurance to Guard against Ransomware Attacks.” *Reuters*, May 19, 2017. https://www.reuters.com/article/us-cyber-attack-insurance/companies-use-kidnap-insurance-to-guard-against-ransomware-attacks-idUSKCN18F1LU.

Beazley. 2018. “Political Violence - Policy Template.”

Boeck, Bill. 2016. “Cyber Attacks and Critical Infrastructure.” Lockton Companies. http://www.lockton.com/whitepapers/Boeck-Cyber_Attacks_and_Critical_Infrastructure_Feb_2016.pdf.

Boonklomjit, Haruethai, Natpakal Rerknithi, Anna Gamvros, and Ruby Kwok. 2018. “Overview of Thailand Draft Personal Data Protection Act.” *Data Protection Report*, August 6, 2018. https://www.dataprotectionreport.com/2018/08/overview-of-thailand-draft-personal-data-protection-act/.

Brandom, Russell. 2017. “Almost All WannaCry Victims Were Running Windows 7.” The Verge. May 19, 2017. https://www.theverge.com/2017/5/19/15665488/wannacry-windows-7-version-xp-patched-victim-statistics.

Buck, Graham. 2018. “Expanding Cyber BI.” Risk & Insurance. March 5, 2018. http://riskandinsurance.com/expanding-cyber-bi/.

Byres, Eric, and Justin Lowe. 2004. “The Myths and Facts behind Cyber Security Risks for Industrial Control Systems.” British Columbia Institute of Technology and PA Consulting Group. https://keatsmoodledevtest.kcl.ac.uk/pluginfile.php/1251665/course/section/414590/byres-myths-and-facts-cyber-security-scada.pdf.

Cambridge Centre for Risk Studies. 2016. “Cyber Exposure Data Schema.” Cyber Accumulation Risk Management. https://www.jbs.cam.ac.uk/faculty-research/centres/centre-for-risk-studies/publications/space-and-technology/cyber-exposure-data-schema/.

Chinn, Menzie D., and Robert W. Fairlie. 2010. “ICT Use in the Developing World: An Analysis of Differences in Computer and Internet Penetration.” *Review of International Economics* 18 (1): 153–67. https://doi.org/10.1111/j.1467-9396.2009.00861.x.

Chirgwin, Richard. 2018. “IT ‘heroes’ Saved Maersk from NotPetya with Ten-Day Reinstallation Bliz.” The Register. January 25, 2018. https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/.

Chris Baraniuk. 2017. “Should You Pay the WannaCry Ransom? - BBC News.” BBC. May 15, 2017. https://www.bbc.co.uk/news/technology-39920269.

Claire. 2016. “How To Cover Electronic Aggression, or Cyberbullying | Improving Public Understanding of Insurance.” Insurance Information Institute. December 12, 2016. http://www.iii.org/insuranceindustryblog/how-to-cover-electronic-aggression-or-cyberbullying/.

Clyde&Co. 2018a. “Cyber and Business Interruption Risks: Connectivity Adds Complexity.” Clyde&Co. https://www.clydeco.com/uploads/Files/J421469_US_Business_Interruption_White_Paper_FV2_FINAL.pdf.

———. 2018b. “FI and D&O International Review.” Clyde&Co. https://www.clydeco.com/uploads/Blogs/insurance/fido-international-review-May-2018.pdf.

CNA. 2018. “Singapore to Pump in S$30m for New Regional Cybersecurity Training Centre.” Channel NewsAsia. September 19, 2018. https://www.channelnewsasia.com/news/singapore/singapore-to-pump-in-s-30m-for-new-regional-cybersecurity-10735308.

Coburn, A. W, J Daffron, A Smith, J Bordeau, E Leverett, S Sweeney, and T Harvey. 2018. “Cyber Risk Outlook 2018.” University of Cambridge: Centre for Risk Studies, University of Cambridge, in collaboration with Risk Management Solutions, Inc. 17 September 2018. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf.

Coburn, Andrew, Eireann Leverett, and Gordon Woo. 2019. *Solving Cyber Risk: Protecting Your Company and Society*. John Wiley & Sons. https://www.amazon.co.uk/Solving-Cyber-Risk-Protecting-Company/dp/1119490936.

Cohn, Carolyn. 2018. “Europe’s New Data Privacy Law Boosts Cyber Insurance Sales.” Insurance Journal. May 22, 2018. https://www.insurancejournal.com/news/international/2018/05/22/489977.htm.

Collins, Keith. 2017. “The Hackers behind the WannaCry Ransomware Attack Have Finally Cashed Out.” Quartz. August 3, 2017. https://qz.com/1045270/wannacry-update-the-hackers-behind-ransomware-attack-finally-cashed-out-about-140000-in-bitcoin/.

Connor, Fred o’. 2017. “NotPetya Still Roils Company’s Finances, Costing Organizations $1.2 Billion in Revenue.” Cybereason. https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue.

Cramer, Stella, Wilson Ang, David Olds, Jessica Paulin, and Jeremy Lua. 2018. “Singapore’s New Cybersecurity Act Comes into Force: Here’s What You Need to Know.” Data Protection Report. September 6, 2018. https://www.dataprotectionreport.com/2018/09/singapores-new-cybersecurity-act-come-into-force-heres-what-you-need-to-know/.

Crowe, Jonathan. 2017. “How One of the World’s Largest Law Firms Was Paralyzed by Petya.” July 2017. https://blog.barkly.com/dla-piper-petya-ransomware-attack.

“Cyber Attack Led to Bristol Airport Blank Screens.” 2018. BBC News. September 16, 2018. https://www.bbc.co.uk/news/uk-england-bristol-45539841.

DAC Beachcroft. 2017. “US Developments in Cyber-Breach D&O Lawsuits.” DAC Beachcroft. February 8, 2017. https://www.dacbeachcroft.com/en/gb/articles/2017/february/us-developments-in-cyber-breach-do-lawsuits.

Dalesio, P. Emery. 2017. “Take down: Hackers Looking to Shut down Factories for Pay.” Phys.Org. August 9, 2017. https://phys.org/news/2017-08-hackers-factories.html.

“Data Protection around the World.” 2018. Commission Nationale de l’Informatique et Des Libertés. May 15, 2018. https://www.cnil.fr/en/data-protection-around-the-world.

Dean, Benjamin. 2018. “An Exploration of Strict Products Liability and the Internet of Things.” *SSRN Electronic Journal*, Center for Democracy & Technology, . https://doi.org/10.2139/ssrn.3193049.

Delta. 2018. “UPDATED: Statement on [24]7.Ai Cyber Incident.” Delta News Hub. April 7, 2018. https://news.delta.com/updated-statement-247ai-cyber-incident.

Delta Insurance. 2018. “The Evolution of Cyber Threats: Embracing Cyber Risk Management.” *Thought Leadership Series*, March 2018, 4 edition. https://deltainsurance.co.nz/wp-content/uploads/2018/02/Delta-Insurance-Cyber-White-Paper.pdf.

Dickey, Colin. 2015. “A Fault in Our Design.” Aeon. https://aeon.co/essays/technological-progress-makes-us-more-vulnerable-to-catastrophe.

“Digital Evolution Index Maps Competitiveness of 60 Countries.” 2017. The Next Silicon Valley. http://www.thenextsiliconvalley.com/2017/07/21/4784-digital-evolution-index-maps-competitiveness-of-60-countries/.

“DLA Piper Global Data Protection Laws of the World - World Map.” n.d. DLA Piper. Accessed September 18, 2018. https://www.dlapiperdataprotection.com/.

DLAPiper. 2017. “Privacy Bill Introduced - Data Protection - New Zealand.” January 24, 2017. http://www.mondaq.com/NewZealand/x/686066/Data+Protection+Privacy/Privacy+Bill+introduced.

“Economic Impact of Cybercrime - No Slowing Down.” 2018. Santa Clara, CA: McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf.

“Estimated Value of Cyber Insurance Premiums Written Worldwide from 2014 to 2020 (in Billion U.S. Dollars).” 2018. Statista. 2018. https://www.statista.com/statistics/533314/estimated-cyber-insurance-premiums/.

Field, Matthew. 2018. “WannaCry Cyber Attack Cost the NHS £92m as 19,000 Appointments Cancelled.” *The Telegraph*, October 11, 2018. https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

Fitch Ratings. 2018. “D&O Liability Carriers May Have a Challenging Year.” Carrier Management. February 25, 2018. https://www.carriermanagement.com/news/2018/02/25/175961.htm.

Gandhi, Prashant, Somesh Khanna, and Sree Ramaswamy. 2016. “Which Industries Are the Most Digital (and Why)?” Harvard Business Review. https://hbr.org/2016/04/a-chart-that-shows-which-industries-are-the-most-digital-and-why#comment-section.

Ghosh, Agamoni. 2017. “WannaCry: List of Major Companies and Networks Hit by Ransomware around the Globe.” *International Business Times*, May 16, 2017. https://www.ibtimes.co.uk/wannacry-list-major-companies-networks-hit-by-deadly-ransomware-around-globe-1621587.

Gibbs, Samuel. 2017. “WannaCry: Hackers Withdraw £108,000 of Bitcoin Ransom.” *The Guardian*, August 3, 2017, sec. Technology. https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom.

Glassman, Mitchell L, and Gordon L Miller. 2016. “Will a Cyberattack Cause the Next Big Bank Failure?” American Banker. June 9, 2016. https://www.americanbanker.com/opinion/will-a-cyberattack-cause-the-next-big-bank-failure.

Goldman, Jeff. 2016. “HSBC Internet Banking Disabled by DDoS Attack.” February 1, 2016. https://www.esecurityplanet.com/network-security/hsbc-internet-banking-disabled-by-ddos-attack.html.

Gottwald, Stephan. 2009. “Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure.” European Commission: Justice, Freedom and Security. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/2009_dependencies_en.pdf.

Graham, Chris. 2017. “NHS Cyber Attack: Everything You Need to Know about ‘biggest Ransomware’ Offensive in History.” The Telegraph. May 20, 2017. https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/.

Greenberg, Andy. 2017. “The WannaCry Ransomware Hackers Made Some Major Mistakes | WIRED.” May 15, 2017. https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/.

———. 2018. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” *Wired*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Hedrich, Wolfram, Gerald Wong, and Jaclyn Yeo. 2017. “Cyber Risk in Asia-Pacific: The Case for Greater Transparency.” Marsh & McLennan. http://www.mmc.com/content/dam/mmc-web/Files/APRC/aprc-cyber-risk-in-asia-pacific.pdf.

Hern, Alex. 2017. “Hacking Risk Leads to Recall of 500,000 Pacemakers Due to Patient Death Fears.” The Guardian. August 31, 2017. https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update.

Hook, Lucy. 2018. “Cyber Claims against Directors and Officers to Rise in 2018, Says Aon Firm Stroz Friedberg.” Insurance Business. January 16, 2018. www.insurancebusinessmag.com/uk/news/cyber/cyber-claims-against-directors-and-officers-to-rise-in-2018-says-aon-firm-stroz-friedberg-89465.aspx.

Huang, Claire. n.d. “Asia Under-Insured against Cyber Threats: Study.” *The Business Times*. Accessed November 17, 2017. http://www.businesstimes.com.sg/technology/asia-under-insured-against-cyber-threats-study.

“Insights Learned from Anatomy of Cyber-Attacks Targeting Banks.” 2016. Innopay analysis. https://innopay.com/blog/insights-learned-from-anatomy-of-cyber-attacks-targeting-banks/.

“Is Cyber Risk Uninsurable? Its 50/50 Says PwC.” 2016. FTSE Global Markets. October 5, 2016. http://www.ftseglobalmarkets.com/news/is-cyber-risk-uninsurable-its-50-50-says-pwc.html.

JLT. 2018a. “Cyber Drives Business Interruption Concerns.” March 1, 2018. http://www.jltspecialty.com/our-insights/publications/cyber-decoder/cyber-drives-business-interruption-concerns.

———. 2018b. “JLT Asia Regional Survey into Cyber Buying Trends.” June 1, 2018. http://www.jltspecialty.com/our-insights/publications/cyber-decoder/jlt-asia-regional-survey-into-cyber-buying-trends.

Joven, Rommel. 2017. “Ransomware-as-a-Service: Rampant in the Underground Black Market.” February 16, 2017. https://www.fortinet.com/blog/threat-research/ransomware-as-a-service-rampant-in-the-underground-black-market.html.

Kearney, Laila. 2018. “Atlanta Officials Reveal Worsening Effects of Cyber Attack.” Reuters. June 6, 2018. https://uk.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUKKCN1J231M.

Kim, Taw. 2018. “Warren Buffett: Cybersecurity Risk ‘Is Uncharted Territory. It’s Going to Get Worse, Not Better.’” CNBC. May 5, 2018. https://www.cnbc.com/2018/05/05/warren-buffett-cybersecurity-risk-is-uncharted-territory-its-going-to-get-worse-not-better.html.

Kollewe, Julia. 2017. “Lloyd’s Says Cyber-Attack Could Cost $120bn, Same as Hurricane Katrina.” The Guardian. https://www.theguardian.com/business/2017/jul/17/lloyds-says-cyber-attack-could-cost-120bn-same-as-hurricane-katrina.

Kovacs, Eduard. 2016. “IBM Reports Significant Increase in ICS Attacks.” Security Week. December 27, 2016. https://www.securityweek.com/ibm-reports-significant-increase-ics-attacks.

Kwang, Kevin. 2017. “Singapore’s Cybersecurity Bill Delayed to 2018.” *Channel NewsAsia*, September 18, 2017. http://www.channelnewsasia.com/news/singapore/singapore-s-cybersecurity-bill-delayed-to-2018-9225622.

Langton, Asher. 2018. “Underground Malware Marketplaces.” Juniper.Net. February 13, 2018. https://forums.juniper.net/t5/Threat-Research/Underground-Malware-Marketplaces/ba-p/318873.

Lenihan, Rob. 2018. “Marsh Launches Enhanced Cyber Risk Solutions for Business Interruption.” *Business Insurance*, April 13, 2018. http://www.businessinsurance.com/article/20180413/NEWS06/912320587/Marsh-launches-suite-of-analytics-enhanced-cyber-risk-solutions-for-business-int.

“Managing Cyber Insurance Accumulation Risk.” 2016. Cambridge, United Kingdom: Cambridge Centre for Risk Studies. https://www.jbs.cam.ac.uk/faculty-research/centres/centre-for-risk-studies/publications/space-and-technology/managing-cyber-insurance-accumulation-risk/.

Marshall, Jacinta Munro, Gordon Archibald,Stan Gallo,Kate. 2017. “Privacy Changes Are Coming – Are You Ready? | KPMG | AU.” KPMG. May 19, 2017. https://home.kpmg.com/au/en/home/insights/2017/05/privacy-act-changes-australian-organisations.html.

McAfee. 2018. “Economic Impact of Cybercrime - No Slowing Down.” Santa Clara, CA: McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf.

McMillan, Robert. 2017. “Tornado-Siren False Alarm Shows Radio-Hacking Risk.” The Wall Street Journal. April 12, 2017. https://www.wsj.com/articles/tornado-siren-false-alarm-shows-radio-hacking-risk-1492042082.

Miller, Mark. 2018. “Cyber Insurance for Business Interruption Losses.” *Miller Friel Insurance Coverage Blog* (blog). July 31, 2018. http://millerfriel.com/blog/cyber-insurance-for-business-interruption-losses/.

Morgan, Steve. 2017. “2018 Cybersecurity Market Report.” Cyber Security Ventures. May 31, 2017. https://cybersecurityventures.com/cybersecurity-market-report/.

Nash, Kim S., Sara Castellanos, and Adam Janofsky. 2018. “One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs.” *Wall Street Journal*, June 27, 2018, sec. Pro Cyber. https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906.

Newman, Lily Hay. 2017. “How an Accidental ‘Kill Swithc’ Slowerd Friday’s Massive Ransomware Attack.” WIRED. May 13, 2017. https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/.

Norton by Symantec. 2018. “2017 Norton Cyber Security Insights Report - Global Results,” 30.

NTU-IRFRC. 2016. “Cyber Risk Management Project (CyRiM).” Winter 2016. http://irfrc.ntu.edu.sg/Research/cyrim/Pages/Home.aspx.

Nunnikhoven, Mark. 2017. “WannaCry & The Reality Of Patching.” Trend Micro Simply Security. May 14, 2017. https://blog.trendmicro.com/wannacry-reality-of-patching/.

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

Office of the Australian Information Commissioner (OAIC). n.d. “Notifiable Data Breaches Scheme.” Accessed September 11, 2018. https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme.

Osborne, Charlie. 2018. “NonPetya Ransomware Forced Maersk to Reinstall 4000 Servers, 45000 PCs.” ZDNet. January 26, 2018. https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/.

Palmer, Danny. 2017. “NotPetya Cyber Attack on TNT Express Cost FedEx $300m.” ZDNet. September 20, 2017. https://www.zdnet.com/article/notpetya-cyber-attack-on-tnt-express-cost-fedex-300m/.

PCS. 2018. “PCS: NotPetya Insured Losses Now $3bn+.” Re-Insurance. 2018. https://www.re-insurance.com/news/pcs-notpetya-insured-losses-now-3bn/1627.article.

Peachey, Kevin. 2016. “HSBC Online Banking Is ‘Attacked.’” BBC. January 29, 2016. https://www.bbc.com/news/business-35438159.

“Percentage of Individuals Using the Internet 2000-2012.” 2013. International Telecommunications Union. http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls.

Perlroth, Nicole. 2017. “Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say.” New York Times. July 6, 2017. https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html.

Privacy International. n.d. “State of Privacy.” Accessed August 22, 2018. https://privacyinternational.org/type-resource/state-privacy.

PwC. 2018. “Insurance 2020 & beyond: Reaping the Dividends of Cyber Resilience.” PwC. 2018. https://www.pwc.com/gx/en/industries/financial-services/publications/insurance-2020-cyber.html.

Ralph, Oliver. 2017. “Should Individuals Buy Insurance against Cyber Attacks?” Financial Times. November 8, 2017. https://www.ft.com/content/72e11ca6-98ad-11e7-8c5c-c8d8fa6961bb.

Ralph, Oliver. 2018. “Cyber Attacks: The Risks of Pricing Digital Cover.” *Financial Times*, March 19, 2018. https://www.ft.com/content/31515a18-238f-11e8-ae48-60d3531b7d11.

“Reforms to Singapore Personal Data Protection Law in Force from 2019.” 2018. Enterprise Innovation | Asia’s Premier Business and Technology Publication. September 9, 2018. https://www.enterpriseinnovation.net/article/reforms-singapore-personal-data-protection-law-force-2019-255872463.

Reidy, Madison. 2018. “Andrew Little Gives More Power to the Privacy Commissioner in New Bill.” Stuff. March 25, 2018. https://www.stuff.co.nz/business/102503447/andrew-little-gives-more-power-to-the-privacy-commissioner-in-new-bill.

Reinsurance. 2017. “Re/Insurance to Take Minimal Share of $8 Billion WannaCry Economic Loss: A.M. Best - Reinsurance News.” *ReinsuranceNe.Ws* (blog). May 23, 2017. https://www.reinsurancene.ws/reinsurance-take-minimal-share-8-billion-wannacry-economic-loss-m-best/.

———. 2018. “Merck’s NotPetya Insured Loss Could Still Be $2bn.” Re-Insurance. November 7, 2018. https://www.re-insurance.com/news/mercks-notpetya-insured-loss-could-still-be-2bn/2142.article.

Reuhs, Nicholas. 2016. “Insurance Coverage for the Internet of (Defective) Things.” Ice Miller LLP. October 27, 2016. https://www.icemiller.com/Ice-on-Fire-Insights/Publications/Insurance-Coverage-for-the-Internet-of-(Defective).

Ruffle, Simon, Eireann Leverett, Andrew Coburn, Jennifer Copic, Scott Kelly, and Tamara Evan. 2015. “Business Blackout - The Insurance Implications of a Cyber Attack on the US Power Grid.” Cambridge, United Kingdom: Centre for Risk Studies, University of Cambridge Judge Business School. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-lloyds-business-blackout-scenario.pdf.

Sacks, Samm. 2018. “China’s Emerging Data Privacy System and GDPR.” *Center for Strategic & International Studies* (blog). March 9, 2018. https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr.

Sayfayn, Nabil, and Stuart Madnick. 2017. “Cybersafety Analysis of the Maroochy Shire Sewage Spill.” Working Paper CISL# 2017-09. Cambridge, MA: Cybersecurity Interdisciplinary Systems Laboratory, Sloan School of Management, Massachusetts Institute of Technology. http://web.mit.edu/smadnick/www/wp/2017-09.pdf.

Schick, Shane. 2017. “Insider Threats Account for Nearly 75 Percent of Security Breach Incidents.” *Security Intelligence* (blog). August 28, 2017. https://securityintelligence.com/news/insider-threats-account-for-nearly-75-percent-of-security-breach-incidents/.

Schiffer, Alex. 2017. “How a Fish Tank Helped Hack a Casino.” Washington Post. July 21, 2017. https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/.

Schneier, Bruce. 2018. *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. 1st ed. W. W. Norton & Company.

SEC.gov. 2018. “Statement on Cybersecurity Interpretive Guidance.” February 2018. https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21.

Smart, William. 2018. “Lessons Learned Review of the WannaCry Ransomware Cyber Attack.” NHS England. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf.

The Law Reviews. 2017. *Japan - The Privacy, Data Protection and Cybersecurity Law Review*. 4th ed. https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151289/japan.

Thompson, Barney. 2017. “DLA Piper Still Struggling with Petya Cyber Attack.” Financial Times. July 6, 2017. https://www.ft.com/content/1b5f863a-624c-11e7-91a7-502f7ee26895.

Trice, Calvin. 2018. “‘Bricked’ Computers Show Cyber Liability Not Always Limited to Digital Assets.” SNL Blogs. *SNL Conference Chatter* (blog). April 24, 2018.

Trilegal. n.d. “The Personal Data Protection Bill, 2018 - Data Protection - India.” Accessed September 11, 2018. http://www.mondaq.com/india/x/727138/data+protection/The+Personal+Data+Protection+Bill+2018.

Turpin, Sarah, and Jeffrey Meagher. 2018. “D&O Insurance for Cyber Liabilities: Increased Cyber Exposure Should Cause Directors & Officers to Take Another Look at Their D&O Policies.” K&L Gates. April 4, 2018. http://www.klgates.com/do-insurance-for-cyber-liabilities-increased-cyber-exposure-should-cause-directors--officers-to-take-another-look-at-their-do-policies-04-04-2018/.

Twersky, Dan. 2015. “Cyber Public Relations Expenses.” Willis Towers Watson Wire. December 18, 2015. https://blog.willis.com/2015/12/cyber-public-relations-expenses/.

UNCTAD. 2016. “Data Protection Regulations and International Data Flows: Implications for Trade and Development.” In , 154.

Vanderburg, Eric. 2018. “Ransomware Developers Learn from the Mistakes of WannaCry, NotPetya.” Carbonite. October 2, 2018. https://www.carbonite.com/blog/article/2017/10/ransomware-developers-learn-from-the-mistakes-of-wannacry-notpetya/.

Wall, Alex. n.d. “Summary: Philippines Data Privacy Act and Implementing Regulations.” Accessed September 11, 2018. https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations/.

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.

Wells, Andrea. 2018. “What Agent Who Wrote First Cyber Policy Thinks About Cyber Insurance Now.” Insurance Journal. March 1, 2018. https://www.insurancejournal.com/news/national/2018/03/01/481886.htm.

Wikipedia. 2017. “WannaCry Ransomware Attack.” *Wikipedia*. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.

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.

Woo, Gordon. 2017. “Reimagining the WannaCry Cyberattack.” RMS. November 30, 2017. https://www.rms.com/blog/2017/11/21/reimagining-the-wannacry-cyberattack/.

World Bank. 2016. “Listed Domestic Companies, Total.” 2016. https://data.worldbank.org/indicator/CM.MKT.LDOM.NO?locations=US.

———. n.d. “World | Intermediate Goods | Exports | to All Country | 2016 | WITS | Data.” Accessed September 12, 2018. https://wits.worldbank.org/CountryProfile/en/Country/WLD/Year/2016/TradeFlow/Export/Partner/all/Product/UNCTAD-SoP2.

World Input Output Database. n.d. “WIOD 2016 Release.” Accessed September 12, 2018. http://www.wiod.org/database/wiots16.

World Shipping Council. n.d. “Trade Statistics | World Shipping Council.” Accessed September 12, 2018. http://www.worldshipping.org/about-the-industry/global-trade/trade-statistics.

Wylie, Ian. 2015. “Danger in the Digital Age: The Internet of Vulnerable Things.” Financial Times. https://www.ft.com/content/fc2570f0-cef4-11e4-b761-00144feab7de.

Yamanouchi, Kelly. n.d. “Lawsuits Target Delta and Vendor for Cybersecurity Breach.” The Atlanta Journal-Constitution. Accessed August 23, 2018. https://www.ajc.com/business/lawsuits-target-delta-and-vendor-for-cybersecurity-breach/nfwNIR8nLm1Sbfv2CwnSqJ/.

Annex A: Global cybercrime

Cyber criminals and their crimes are growing in maturity, complexity and, as a result, impact. Over 6,000 online criminal marketplaces now sell commercialised and easily-accessible ransomware products and services, amongst other malware types, offering over 45,000 different products.[104] WannaCry, a virulent and vicious ransomware worm released in 2017, cost upwards of $4 billion globally. A few months later, NotPetya cost organisations $10 billion in revenue. These types of malware are now readily available online; users can purchase ransomware-as-a-service (RaaS) with a range of pricing models[105] and prices as low as $9.95,[106] and there is a plethora of free tutorials and open-source code available for intrepid cyber criminals. Future losses from large-scale cyberattacks, both economic and insured, are forecasted in the billions of dollars.[107]

Losses from cybercrime have been reported in almost every industrialised nation, but accurately quantifying these losses is challenging. Victims are often unwilling to share breach statistics and internal loss estimates can be inaccurate or incomplete due to the complexities of reputation damage, clean-up costs and lost revenue. Furthermore, it is difficult to price the loss of intellectual property, confidential business information, and potential revenue or productivity due to business disruption. Personal identifiable information is often valued by the price it is sold for on the black market rather than the actual loss of that information to the company storing it.

Reported estimates of the cost of cybercrime range from the millions to trillions of dollars. Such an imprecise range is a clear indication that data standards for reporting cybercrime losses require normalisation. The Cambridge Centre for Risk Studies estimates that cybercrime led to losses of $1.5 trillion in 2017.[108]

Global

Cybercrime is not evenly distributed across the world. Concentrations of wealth, percentage of internet users, levels of cyber security infrastructure, e-commerce penetration, and distribution of market sectors as well as a host of other variables have an impact on the potential for, and the reality of, cybercrime.

The financial costs are greatest in wealthy regions that have the greatest potential for loss and, for the cyber criminals, higher financial pay-outs and disruption potential. Increased connectivity and reliance on technology within a population or company also increases the probability of cyberattacks. The highest costs are seen in North America, Europe and Central Asia where the percentage of individuals using the internet ranges between 80 and 97%.[109]

[104] McAfee 2018

[105] Langton 2018

[106] Joven 2017

[107] Kollewe 2017

[108] A. Coburn, Leverett, and Woo 2019

[109] “Percentage of Individuals Using the Internet 2000-2012” 2013

Table 14: The regional distribution of the cost of cybercrime[110]

Region (World Bank)	Region GDP ($US, trillion)	Cybercrime Cost ($US, billion)	Cybercrime Loss (% GDP)
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America and the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
Middle East and North Africa (MENA)	3.1	2 to 5	0.06 to 0.16%
World	$75.8	$445 to $608	0.59 to 0.80%

The Digital Evolution Index (DEI) [111] scores countries based on policies to advance digital strategies and pace of change in digital progression. Singapore sits at 6th place, indicating its high level of digitisation and continued innovation. The countries in the top 10 places, listed in order, are Norway, Sweden, Switzerland, Denmark, Finland, Singapore, South Korea, UK, Hong Kong, and the US.

Table 15: Countries ranked by their Digital Evolution Index

Country	Rank	Country	Rank	Country	Rank
Norway	1	Australia	11	Estonia	21
Sweden	2	Canada	12	UAE	22
Switzerland	3	Netherlands	13	Israel	23
Denmark	4	New Zealand	14	Portugal	24
Finland	5	Japan	15	Spain	25
Singapore	6	Ireland	16	Malaysia	26
South Korea	7	Germany	17	Czech Republic	27
UK	8	Belgium	18	Latvia	28
Hong Kong	9	Austria	19	Slovenia	29
US	10	France	20	Chile	30
Saudi Arabia	31	Bulgaria	41	Philippines	51
Hungary	32	Thailand	42	Kenya	52
Slovak Republic	33	South Africa	43	India	53
Italy	34	Colombia	44	Egypt	54
Poland	35	Indonesia	45	Nigeria	55
China	36	Brazil	46	Pakistan	56
Turkey	37	Mexico	47	Algeria	57
Greece	38	Vietnam	48	Cameroon	58
Russia	39	Peru	49	Bolivia	59
Jordan	40	Morocco	50	Bangladesh	60

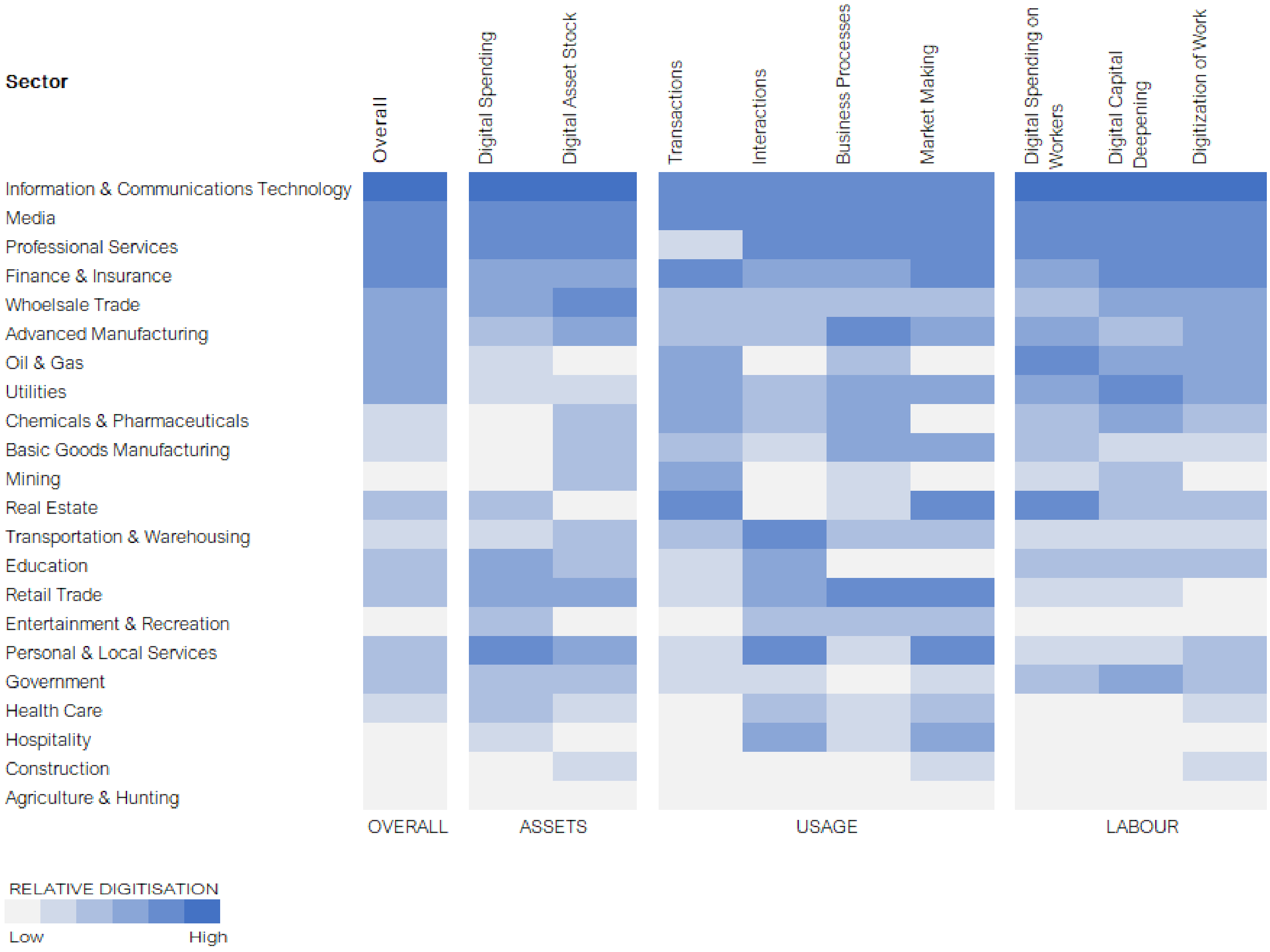
[110] “Economic Impact of Cybercrime - No Slowing Down” 2018

[111] “Digital Evolution Index Maps Competitiveness of 60 Countries” 2017

Sectoral

Similar to the distribution across countries, the distribution of cybercrime across sectors is varied according to potential for loss and connected dependencies. Underlying business processes have become increasingly connected across all sectors. In retail some brands have seamlessly integrated customer services and social media platforms in their physical stores.

Figure 6: Level of digitalisation across sectors[112]



Source: 'Which Industries are the Most Digital and why?' Harvard Business Review

The variation across sectors is directly related to the dependence of each sector on connected devices for business revenue and management. Relative digitisation of industries is measured according to the level of hardware, software, data, and IT service investments along with the digitisation of physical assets such as big data systems in supply chains, connected vehicle fleets, smart buildings etc.

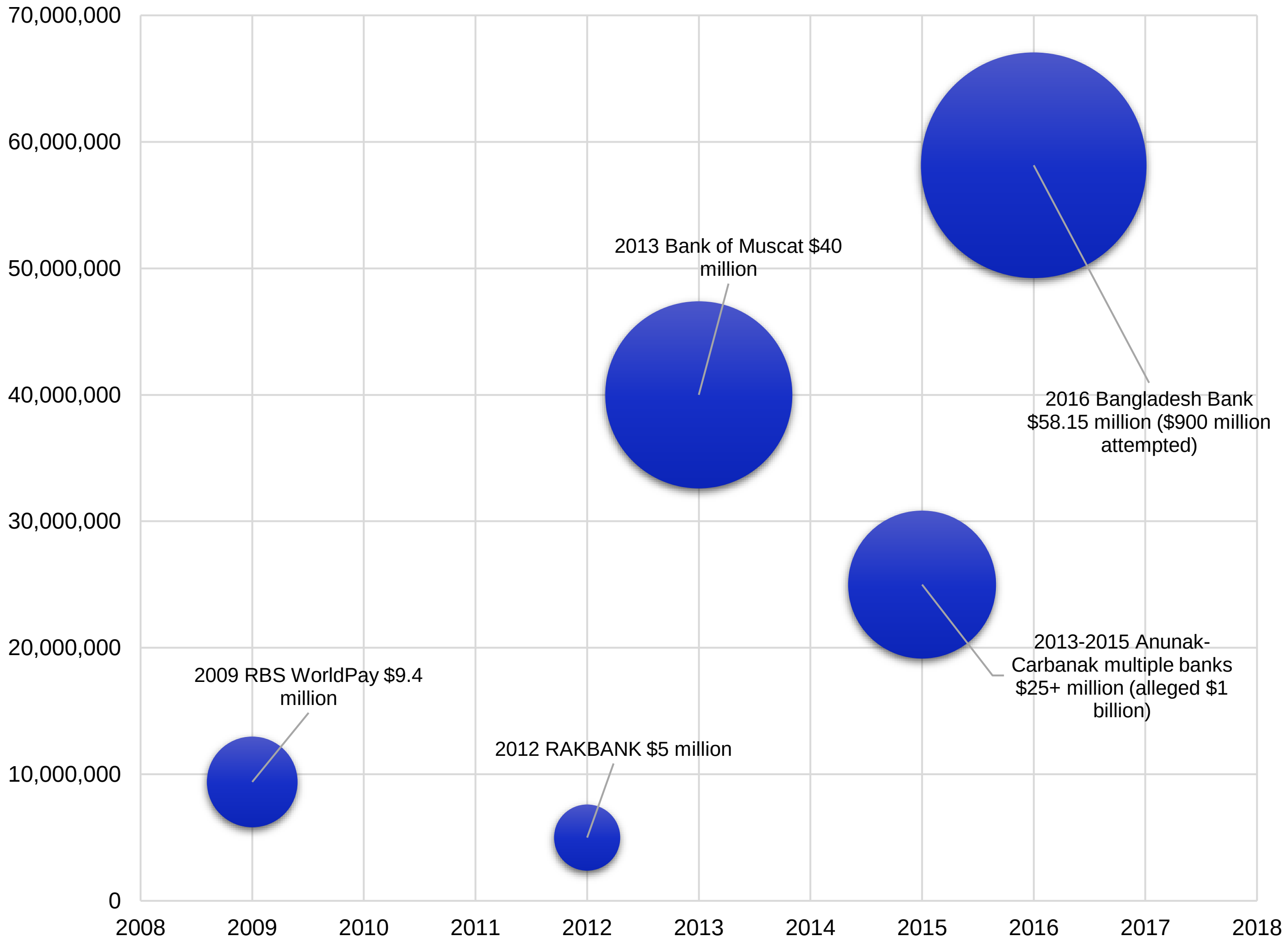
[112] Original research and analysis by the McKinsey Global Institute (Gandhi, Khanna, and Ramaswamy 2016)

Area of interest: Finance

Concentrations of losses are often seen in the financial sector where banks are the targets of skilled cyber criminals. Cyber security professionals report that financial institutions spend three times as much on cybersecurity as nonfinancial institutions[113] and there have been several high-profile, expensive cyber bank heists in the last decade.

Financial motivations are not the only drivers of attacks against the finance industry. Sometimes disruption is the primary goal of the attackers rather than theft. In April 2018, seven of the largest banking institutions in the UK, including Tesco Bank, Royal Bank of Scotland, and Santander, were targeted by coordinated cyberattacks, forcing them to reduce operations and, in some cases, shut down entire systems. The National Crime Agency put the damage in the range of hundreds of thousands of pounds. In January 2016, on a payday Friday and two days before the deadline for tax returns, the HSBC online banking and digital services portal suffered a DDoS attack[114] that disrupted personal banking services for customers for several hours.[115]

Figure 7: Publicly known major banking cybercrime losses, $ millions (not an exhaustive list)[116]



[113] "Things to do before the next big thing: How the financial industry reacts to cyberthreats," Kaspersky, March 9, 2017

[114] Peachey 2016

[115] Goldman 2016

[116] "Insights Learned from Anatomy of Cyber-Attacks Targeting Banks" 2016

Area of interest: Industrial control systems

IBM reports that cyberattacks on industrial control systems (ICS) increased 110% in 2016[117] and 636% from 2012 to 2014.[118] ICS oversee smart grids, nuclear power plants, water and waste treatment plants, electric power plants,[119] air traffic control, transportation, manufacturing facilities, chemical plants and many other critical infrastructures (CI). These important functions make them frequent targets, with 15% of cyberattacks involving the destruction of physical assets such as routers, servers, storage devices, or ICS.[120]

Malware attacks on ICS such as Black Energy, StoneDrill, Stuxnet, Duqu, Shamoon, and Havex have been well-documented,[121] with many focusing on compromising the standard control-layer protocols used in ICS and by operational technology vendors. Famous targets include a small dam in the US, a water and sewage system in Australia, a railway system in the US, a steel mill in Germany, an oil pipeline in Turkey, and the power grid in Ukraine.[122] In 2017, a new ICS-specific malware, CrashOverride, disrupted electricity grid operations in Ukraine, showing that malware could target safety instrumented systems (SIS) and pose a legitimate hazard to human life.[123] Targeting SIS can lead to loss of physical property damage, extensive system downtime, and other dangerous impacts such as false safety alarms.[124]

[117] Kovacs 2016

[118] Sayfayn and Madnick 2017

[119] Perlroth 2017

[120] Wylie 2015

[121] Byres and Lowe 2004

[122] Boeck 2016

[123] Ashford 2018; Schneier 2018

[124] McMillan 2017

Annex B: Cyber scenario selection

This collaborative project between Cambridge Centre for Risk Studies (CCRS) and CyRiM will result in two cyber catastrophe scenario reports, the first of which is presented in this document. These scenarios are realistic, low probability, high impact events. Understanding the impact of severe events is one of the key requirements for insurers to develop cyber risk cover.

Through research, workshop development, and expert elicitation CCRS proposed eleven potential scenarios that were narrowed down to six for potential development. A workshop held in Singapore attended by insurance and technology industry experts analysed and discussed the following five scenarios in addition to 'Global infection by contagious malware' to be considered for report development:

1. ICS-Triggered Fires in Refineries. Cyber criminals target the electronic-based measurement and management devices of the Industrial Control Systems within oil refineries resulting in simultaneous systems errors and explosions.
2. Flash Crash of Asia-Pacific Stock Exchanges. Cyber criminals target the trading platforms used by institution traders for executing trades and algorithmic trading. The criminals initiate a fire sale of various equities and FX positions. High-frequency trading algorithms are also altered, amplifying the volatility of the stock market.
3. Cyber-Attack on Smart Nation Infrastructure. Cyber criminals target centralised smart power grids, water treatment facilities, ICS, communication and internet systems involved in the smart nation infrastructure, shutting them down and preventing access by to all citizens.
4. Data Exfiltration Targets Mobiles. Advanced hacking techniques allow cyber criminals to remotely exploit a chip vulnerability which allows access to kernel-level memory without proper security checks. The Android mobile phone operating system is targeted. All cached memory is accessed - banking details and intellectual property are the specified targets. Criminals access banking apps to drain accounts and sell on bank details and intellectual property. Results in largest data exfiltration event.
5. Cyber-Attack on Multiple Port Management Systems. Cyber criminals target the port management software that allows users to manage, plan, and view actions taking place, and permits information to be shared across stakeholders, including terminals, ship handlers, government officials, etc. The inventory is corrupted over several months to facilitate theft of cargo on a large scale. Criminals encrypt the cargo inventories when discovered.

After consideration by the attendees of the workshop in Singapore and the CyRiM advisory board, the 'Global infection by contagious malware' scenario developed in this report and 'Cyber-attack on multiple port management systems' were chosen for report creation and loss estimation.

Annex C: X1 variant

Figure 8: X1 Total direct and indirect economic losses from business interruption by sector, $ billion

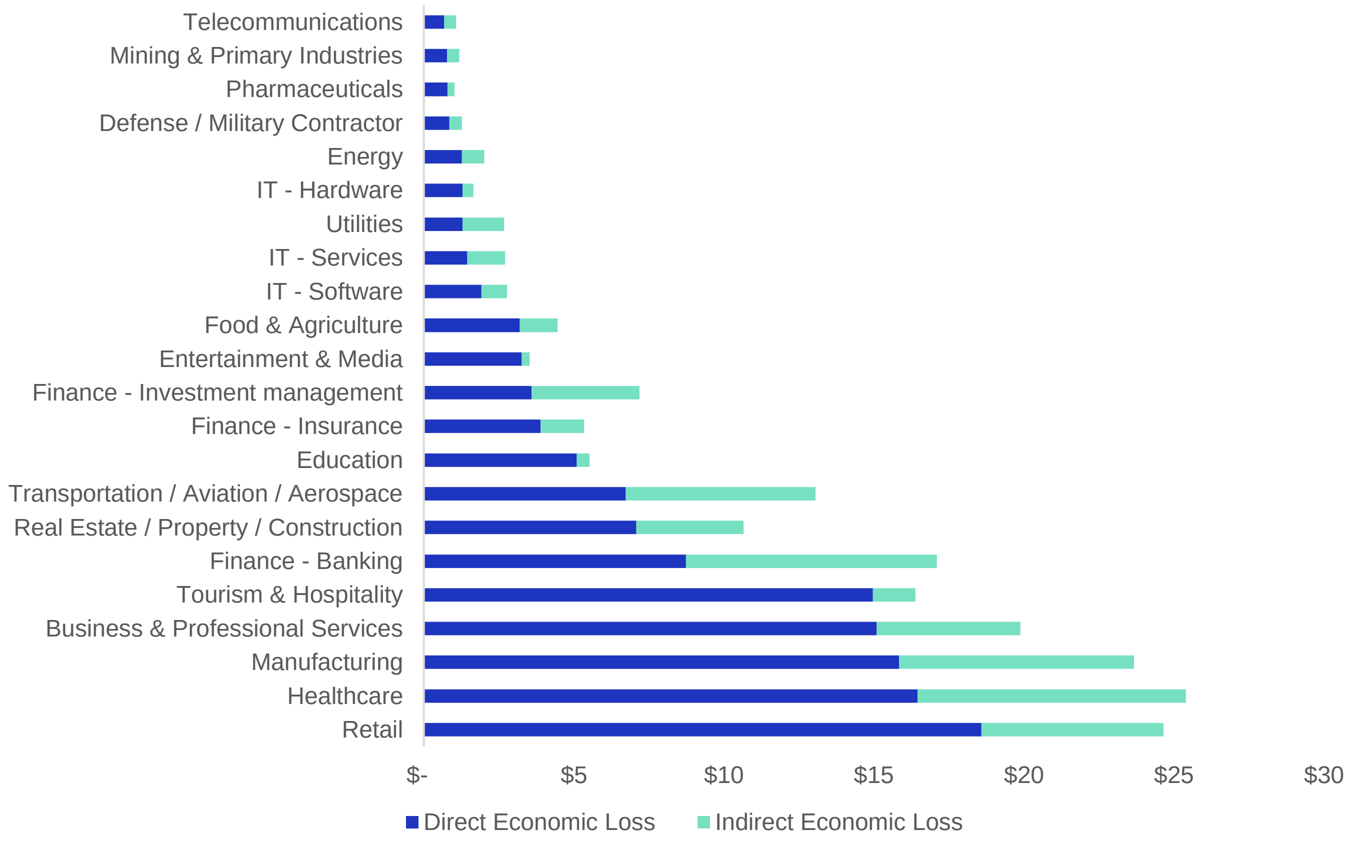


Figure 9: Distribution of direct economic loss (productivity and consumption loss only) in X1 by sectors and regions

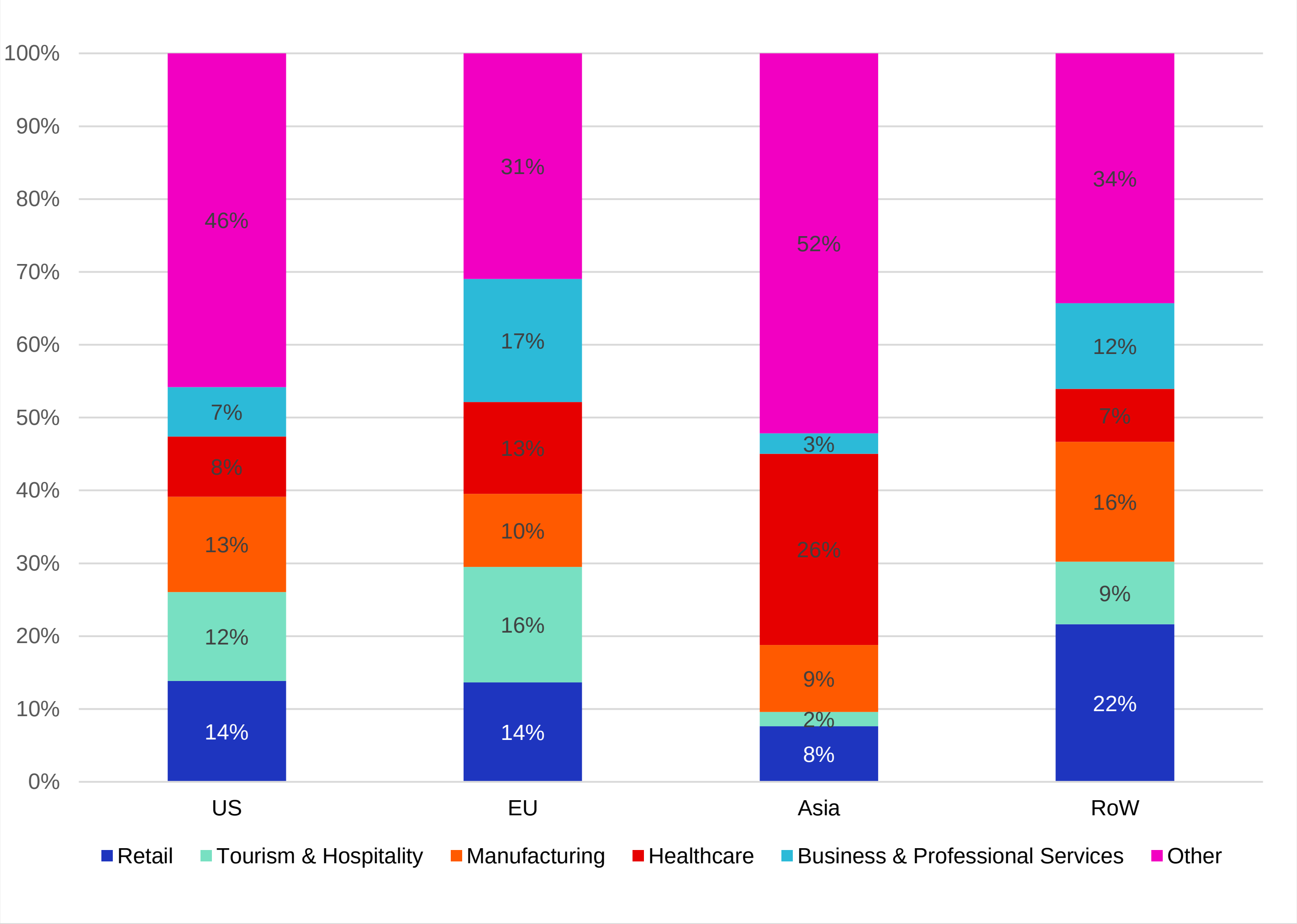


Table 16: Infection rate by size and sector for X1

Sector	Premier	Small	Medium	Large
Business & Professional Services	12%	8%	8%	11%
Defense / Military Contractor	6%	5%	4%	4%
Education	21%	15%	15%	20%
Energy	8%	6%	6%	8%
Entertainment & Media	15%	10%	10%	14%
Finance - Banking	21%	15%	15%	20%
Finance - Insurance	14%	10%	10%	14%
Finance - Investment Management	14%	10%	10%	14%
Food & Agriculture	9%	6%	6%	8%
Healthcare	14%	10%	10%	14%
IT - Hardware	18%	10%	10%	13%
IT - Services	17%	11%	10%	14%
IT - Software	14%	10%	10%	14%
Manufacturing	14%	10%	10%	14%
Mining & Primary Industries	6%	3%	3%	4%
Pharmaceuticals	6%	4%	3%	4%
Real Estate / Property / Construction	14%	10%	10%	14%
Retail	16%	11%	11%	15%
Telecommunications	11%	7%	6%	8%
Tourism & Hospitality	10%	8%	8%	11%
Transportation / Aviation / Aerospace	15%	10%	10%	14%
Utilities	8%	6%	6%	8%

Appendix: Guide to insurance portfolio loss

This guide provides the University of Cambridge Centre for Risk Studies' recommended guidelines for insurance companies to estimate losses from the 'Bashe attack: Global infection by malicious malware' scenario. Each subsection outlines the methodology and data required to estimate the insured loss for a particular cyber affirmative and non-affirmative coverage to aid in the estimation of an insurance portfolio. This portfolio estimation method is consistent with the industry loss estimation outlined in the report.

Expected loss calculation

This report details an expected loss calculation as opposed to a rank/selection calculation. For this expected loss calculation, you assume that all your accounts within a specific type of coverage being modelled have a loss given the probability of the incident rate or in this case an infection rate.

Companies directly impacted

Use the infection rates by scenario variants in Table 17, Table 18, and Table 19 and by business sector and company size as multipliers to the loss value ($) for each coverage type detailed below. You will find a concordance table of our sector categories into NAICS 2012 at the end of the section.

Table17: Infection rates by sector and company size for the S1 variant

Sector	SVS	Premier	Large	Medium	Small
Business & Professional Services	3	4%	3%	3%	4%
Defense / Military Contractor	1	3%	3%	3%	2%
Education	5	9%	6%	6%	8%
Energy	2	5%	2%	2%	3%
Entertainment & Media	4	7%	4%	4%	5%
Finance - Banking	5	7%	6%	6%	8%
Finance - Insurance	4	6%	4%	4%	5%
Finance - Investment Management	4	6%	4%	4%	5%
Food & Agriculture	2	3%	2%	2%	3%
Healthcare	4	6%	4%	4%	5%
IT - Hardware	4	7%	4%	4%	5%
IT - Services	4	7%	4%	4%	5%
IT - Software	4	5%	4%	4%	5%
Manufacturing	4	5%	4%	4%	5%
Mining & Primary Industries	1	4%	1%	1%	2%
Pharmaceuticals	1	4%	3%	1%	2%
Real Estate / Property / Construction	4	6%	4%	4%	5%
Retail	5	8%	6%	6%	8%
Telecommunications	2	4%	3%	2%	3%

Tourism & Hospitality	3	5%	3%	3%	4%
Transportation / Aviation / Aerospace	4	5%	4%	4%	5%
Utilities	2	4%	2%	2%	3%

Table 18: Infection rates by sector and company size for the S2 variant

Sector	Premier	Small	Medium	Large
Business & Professional Services	8%	8%	6%	6%
Defense / Military Contractor	6%	3%	4%	4%
Education	16%	15%	11%	11%
Energy	6%	6%	5%	5%
Entertainment & Media	10%	10%	8%	8%
Finance - Banking	16%	15%	11%	11%
Finance - Insurance	10%	10%	8%	8%
Finance - Investment Management	11%	10%	8%	8%
Food & Agriculture	6%	6%	5%	5%
Healthcare	11%	10%	8%	8%
IT - Hardware	12%	10%	8%	8%
IT - Services	11%	10%	8%	8%
IT - Software	10%	10%	8%	8%
Manufacturing	10%	10%	8%	8%
Mining & Primary Industries	5%	3%	2%	2%
Pharmaceuticals	6%	3%	2%	3%
Real Estate / Property / Construction	11%	10%	8%	8%
Retail	14%	13%	10%	10%
Telecommunications	8%	6%	5%	5%
Tourism & Hospitality	9%	8%	6%	6%
Transportation / Aviation / Aerospace	10%	10%	8%	8%
Utilities	7%	6%	5%	5%

Table 19: Infection rates by sector and company size for the X1 variant

Sector	Premier	Small	Medium	Large
Business & Professional Services	12%	8%	8%	11%
Defense / Military Contractor	6%	5%	4%	4%
Education	21%	15%	15%	20%
Energy	8%	6%	6%	8%
Entertainment & Media	15%	10%	10%	14%
Finance - Banking	21%	15%	15%	20%
Finance - Insurance	14%	10%	10%	14%
Finance - Investment Management	14%	10%	10%	14%
Food & Agriculture	9%	6%	6%	8%
Healthcare	14%	10%	10%	14%
IT - Hardware	18%	10%	10%	13%
IT - Services	17%	11%	10%	14%

IT - Software	14%	10%	10%	14%
Manufacturing	14%	10%	10%	14%
Mining & Primary Industries	6%	3%	3%	4%
Pharmaceuticals	6%	4%	3%	4%
Real Estate / Property / Construction	14%	10%	10%	14%
Retail	16%	11%	11%	15%
Telecommunications	11%	7%	6%	8%
Tourism & Hospitality	10%	8%	8%	11%
Transportation / Aviation / Aerospace	15%	10%	10%	14%
Utilities	8%	6%	6%	8%

Business interruption – affirmative cyber

Identify the policies in your portfolio with affirmative cyber business interruption cover[125]. Bucket these policies by sector and assign a sectoral vulnerability score (SVS) as outlined in Table 3 (from the Scenario Variants Section 3). [126] Assume a distribution of internal replication for policies within each business sector as outlined in Table 20. For example, the Pharmaceuticals sector has a SVS score of 1, which means that of all infected policies identified within that sector, 35% of companies suffer a replication rate of between 0-10%. These replication rate buckets are tied to the decay functions for the revenue loss shown in Table 21.

Table 20: Distribution of replication rates by sectoral vulnerability score

SVS	0-10%	10-20%	20-30%	30-40%	40%+
1	35%	45%	10%	7%	3%
2	30%	42%	10%	12%	6%
3	25%	39%	10%	17%	9%
4	20%	36%	10%	22%	12%
5	15%	33%	10%	27%	15%

The severity and duration of business interruption per policy is determined by the replication rate category as outlined in Table 20. Using the Pharmaceuticals example, 35% of policies that are within the replication rate bucket of between 0-10% suffer 5% revenue loss due to BI for the first five days after initial infection, 3% loss due to BI for the next five days, 1% for the next five days and so on.

Table 21: Decay function of revenue loss severity and duration by replication bucket

Number of Business Interruption days	0%-10%	10%-20%	20%-30%	30%-40%	40%+
1 to 5	5%	15%	25%	35%	50%
5 to 10	3%	9%	18%	28%	45%
10 to 15	1%	5%	9%	14%	23%
15 to 20	1%	2%	4%	7%	11%
20 to 25	0%	1%	2%	4%	6%
25 to 30	0%	1%	1%	2%	3%

For this calculation, you will need to know the annual revenue (converted into days) for each account selected. To determine the pay-out, take the projected gross margin for each selected account and multiply this by the amount of revenue lost.

Apply appropriate deductibles and limits for the business interruption, as per the policy terms for these accounts, and calculate the total business interruption loss for your portfolio.

[125] Affirmative cyber BI cover is provided either by a standalone cyber policy or endorsements on a traditional policy.

[126] To convert CCRS sector classifications into the North American Industrial Coding System (NAICS), please see Table 27

Finally, to estimate the expected loss, take the loss value calculated for each BI policy and multiple it by the respective infection rate provided in Table 17, Table 18, and Table 19 given the business sector and company size of the account holder and by 67%. We use 67% as the per cent of policies that file a claim under an affirmative cyber policy.

Business interruption – non-affirmative cyber

Follow the same process outlined above for your traditional property BI[127] policies by substituting the final multiplier of 67% with 33%. We use 33% as the percent of policies that file a claim which could potentially fall under a traditional property BI policy, thus creating non-affirmative cyber exposure.

Cyber extortion

Identify the policies with affirmative cyber extortion cover and assume that these policies pay an average ransom of $700 per infected device to decrypt the data. Not all the devices at a company are infected and not all of the infected devices are decrypted via a ransom payment. Assume a distribution of replication rates across all cyber extortion policies using the data from Table 22 and multiply this by the number of devices at each company, which is typically captured on the insurance applications questionnaires. If the number of devices at a given company is not known, then use the average number of devices by size of the company provided in Table 23. Then assume that of those devices infected, an average of 4% of those devices are decrypted by paying the ransom and multiply this number by the $700 ransom cost.

Depending on the wording in your Kidnap and Ransom policies, you may need to include these policies along with the affirmative cyber extortion policies when selecting policies to apply losses to.

Table 22: Average replication rate distribution for all scenario variants

Percent devices infected	5%	15%	25%	35%	50%
Percent of companies that fall under bucket	25%	39%	10%	17%	9%

Table 23: Distribution of average number of devices per size of company

Size	Average number of devices per size of company
Small	180
Medium	900
Large	3750
Premier	9000

Apply appropriate policy terms for these accounts and calculate the total cyber extortion loss for your portfolio.

Finally, to estimate the expected loss, take the loss value calculated for each cyber extortion policy and multiple it by the respective infection rate provided in Table 17, Table 18 and Table 19, given the business sector and company size of the account holder.

Incident response costs

Identify the policies with affirmative cyber incident response costs and assume that they spend $350 per computer to support forensic investigation activities to assess the extent of damage following the infection and to clean-up the computer. Take the total of number computers for a given account, subtract the number of computers where ransom is paid based on the calculation above, and assume incident response costs are applied to remaining devices.

Apply appropriate policy terms for these accounts and calculate the total incident response cost loss for your portfolio. Finally, to estimate the expected loss, take the loss value calculated for each cyber incident response costs policy and multiple it by the respective infection rate provided in Table 17, Table 18, and Table 19 given the business sector and company size of the account holder.

[127] Traditional property policies that do not explicitly cover cyber or that have potential gaps in their exclusions could create non-affirmative exposure. See Section 6 for more details on the difference between affirmative and non-affirmative exposures.

Data and software loss

For the X1 scenario variant only, identify the policies with affirmative cyber data and software loss cover and assume that they spend $500 per computer to recreate key data that was not recovered. Assume that they do this on 5 key computers at each company.

Apply appropriate policy terms for these accounts and calculate the total data and software cost loss for your portfolio.

Finally, to estimate the expected loss, take the loss value calculated for each cyber data and software loss policy and multiple it by the respective infection rate provided in Table 17, Table 18, and Table 19 given the business sector and company size of the account holder.

Liability (directors & officers)

Identify the policies with either affirmative cyber directors & officers (D&O) cover or traditional D&O cover that support cyber named perils. Identify the market capitalisation valuation for each company and make an assumption of loss.

For cases where market capitalisation is not available make an assumption of loss by company size.

Apply appropriate policy terms, including deductible and limits for these accounts and calculate the total liability loss for companies directly impacted by the malware.

Make an assumption of the probability that the shareholders sue the company. This may vary by scenario size. Finally, to estimate the expected loss, take the loss value calculated for each D&O policy and multiple it by the respective infection rate provided in Table 17, Table 18, and Table 19 given the business sector and company size of the account holder and by the % that are likely to have lawsuits.

The above is one of the possible approach to calculate Liability (directors & officers) losses and in practice the impact will depend on court cases, legal interpretations and it is highly uncertain.

Companies indirectly impacted

Contingent business interruption

Identify the policies in your portfolio with affirmative cyber contingent business interruption (CBI) cover and assume that all of these policies are impacted, and experience supply chain outages based on the distribution shown in Table 24. For example, 18% of all your CBI policies will have 2.5-day outage with only a 45% revenue loss in the S1 scenario variant.

Table 24: Contingent Business Interruption impact

Average BI Days	% of Companies Impacted	% Revenue Impact per Company
2.5	18%	45%
7.5	14%	32%
12.5	7%	16%
17.5	4%	8%
22.5	2%	4%
27.5	1%	2%

Apply appropriate policy terms, including deductible and limits for these accounts and calculate the total CBI loss for companies indirectly impacted by the malware.

Based on CCRS modelling, we estimate that 45% of companies are likely to be impacted indirectly from the Contagious Malware scenario. Finally, to estimate the expected loss, take the loss value calculated for each CBI policy and multiple it by one minus the infection rates[128] provided in Table 17, Table 18, and Table 19 given the business sector and company size of the account holder and by 45%.

[128] CCRS recommend one minus the infection rate to determine the percent of companies that are not directly infected by the malware.

Liability (directors and officers)

Identify the policies with either affirmative cyber D&O cover or traditional D&O cover. Identify the market capitalisation valuation for each company and make an assumption of loss

For cases where market capitalisation is not available make an assumption of loss by company size.

Apply appropriate policy terms, including deductible and limits for these accounts and calculate the total liability loss for companies indirectly impacted by the malware.

Make an assumption of the probability that the shareholders sue the company. This may vary by scenario size. Finally, to estimate the expected loss, take the loss value calculated for each D&O policy and multiple it by the respective infection rate provided in Table 17, Table 18, and Table 19 given the business sector and company size of the account holder and by the % that are likely to have lawsuits.

The above is one of the possible approach to calculate Liability (directors & officers) losses and in practice the impact will depend on court cases, legal interpretations and it is highly uncertain.

Defendant companies

Liability (technology errors and omissions)

Identify all the policies in your portfolio that you insure for technology errors and omissions (TechE&O) or professional liability within the following sector categories shown in Table 25. Select all of these accounts as ‘defendant companies’ in this scenario.

Table 25: Types of companies selected as defendant companies

Company Type	NAICS
IT Services	518210 Data Processing, Hosting and Related Services
	519130 Internet publishing and Broadcasting Web Search Portals
	541511 Custom Computer Programming Services

For each of the selected ‘defendant company’ accounts, assume that they are found liable for the following amounts shown in Table 26 by company size.

Table 26: TechE&O liability per company, $ million

Premier	Large	Medium	Small
$48	$16	$5	$3

Apply appropriate deductibles and limits for the liabilities, as per the policy terms for these accounts, and calculate the total liability loss to defendant companies in your portfolio.

Assume that there is a 1% chance of a lawsuit in S1, 2% for S2 and 10% for X1. Finally, to estimate the expected loss, take the loss value calculated for each TechE&O policy and multiple it by the % that are likely to have lawsuits.

Total

Total all the components of loss into a grand total of losses for your portfolio.

Supporting tables

Table 27 provides a mapping of NAICS 2012 codes to the CRS business sectors. Concordance tables that map other coding systems, such as SIC and GICS and other editions of NAICS to the NAICS 2012, can be found online here.

Table 27: Mapping of Business Sectors to NAICS 2012

Business Sector Coding	Business Sector	NAICS 2012 (Branches Included)	Short Description
1.1	IT - Software	5112	Software Publishers
1.2	IT - Hardware	3341	Computer and Peripheral Equipment Manufacturing
1.3	IT - Services	518	Data Processing, Hosting, and Related Services
1.3	IT - Services	519130	Internet Publishing and Broadcasting and Web Search Portals
1.3	IT - Services	5415	Computer Systems Design and Related Services
2	Retail	42[129]	Wholesale Trade
2	Retail	441	Motor Vehicle and Parts Dealers
2	Retail	442	Furniture and Home Furnishings Stores
2	Retail	443	Electronics and Appliance Stores
2	Retail	444	Building Material and Garden Equipment and Supplies Dealers
2	Retail	445	Food and Beverage Stores
2	Retail	446	Health and Personal Care Stores
2	Retail	447	Gasoline Stations
2	Retail	448	Clothing and Clothing Accessories Stores
2	Retail	451	Sporting Goods, Hobby, Musical Instrument, and Book Stores
2	Retail	452	General Merchandise Stores
2	Retail	453	Miscellaneous Store Retailers
2	Retail	454	Non-store Retailers
3.1	Finance - Banking	521	Monetary Authorities-Central Bank
3.1	Finance - Banking	522	Credit Intermediation and Related Activities
3.2	Finance - Insurance	524	Insurance Carriers and Related Activities
3.3	Finance - Investment management	523	Securities, Commodity Contracts, and Other Financial Investments and Related Activities
3.3	Finance - Investment management	525	Funds, Trusts, and Other Financial Vehicles
4	Healthcare	62	Health Care and Social Assistance
5	Business & Professional Services	5411	Legal Services
5	Business & Professional Services	5412	Accounting, Tax Preparation, Bookkeeping, and Payroll Services
5	Business & Professional Services	5413	Architectural, Engineering, and Related Services
5	Business & Professional Services	5414	Specialized Design Services
5	Business & Professional Services	5416	Management, Scientific, and Technical Consulting Services
5	Business & Professional Services	5417	Scientific Research and Development Services
5	Business & Professional Services	5418	Advertising, Public Relations, and Related Services
5	Business & Professional Services	5419	Other Professional, Scientific, and Technical Services
5	Business & Professional Services	55	Management of Companies and Enterprises
5	Business & Professional Services	561	Administrative and Support Services

[129] All of level 42 is in the Retail sector except for the 2 sub-levels pulled out for Energy (424710 and 424720).

6	Energy	211	Oil and Gas Extraction
6	Energy	213111	Drilling Oil and Gas Wells
6	Energy	213112	Support Activities for Oil and Gas Operations
6	Energy	324	Petroleum and Coal Products Manufacturing
6	Energy	424710	Petroleum Bulk Stations and Terminals
6	Energy	424720	Petroleum and Petroleum Products Merchant Wholesalers (except Bulk Stations and Terminals)
6	Energy	486	Pipeline Transportation
7	Telecommunications	517	Telecommunications
8	Utilities	22	Utilities
8	Utilities	562	Waste Management and Remediation Services
9	Tourism & Hospitality	72	Accommodation and Food Services
10	Manufacturing	313	Textile Mills
10	Manufacturing	314	Textile Product Mills
10	Manufacturing	315	Apparel Manufacturing
10	Manufacturing	316	Leather and Allied Product Manufacturing
10	Manufacturing	321	Wood Product Manufacturing
10	Manufacturing	322	Paper Manufacturing
10	Manufacturing	323	Printing and Related Support Activities
10	Manufacturing	3251	Basic Chemical Manufacturing
10	Manufacturing	3252	Resin, Synthetic Rubber, and Artificial Synthetic Fibers and Filaments Manufacturing
10	Manufacturing	3253	Pesticide, Fertilizer, and Other Agricultural Chemical Manufacturing
10	Manufacturing	3255	Paint, Coating, and Adhesive Manufacturing
10	Manufacturing	3256	Soap, Cleaning Compound, and Toilet Preparation Manufacturing
10	Manufacturing	3259	Other Chemical Product and Preparation Manufacturing
10	Manufacturing	326	Plastics and Rubber Products Manufacturing
10	Manufacturing	327	Nonmetallic Mineral Product Manufacturing
10	Manufacturing	331	Primary Metal Manufacturing
10	Manufacturing	332	Fabricated Metal Product Manufacturing
10	Manufacturing	333	Machinery Manufacturing
10	Manufacturing	3342	Communications Equipment Manufacturing
10	Manufacturing	3343	Audio and Video Equipment Manufacturing
10	Manufacturing	3344	Semiconductor and Other Electronic Component Manufacturing
10	Manufacturing	334510	Electromedical and Electrotherapeutic Apparatus Manufacturing
10	Manufacturing	334512	Automatic Environmental Control Manufacturing for Residential, Commercial, and Appliance Use
10	Manufacturing	334513	Instruments and Related Products Manufacturing for Measuring, Displaying, and Controlling Industrial Process Variables
10	Manufacturing	334514	Totalizing Fluid Meter and Counting Device Manufacturing
10	Manufacturing	334515	Instrument Manufacturing for Measuring and Testing Electricity and Electrical Signals
10	Manufacturing	334516	Analytical Laboratory Instrument Manufacturing
10	Manufacturing	334517	Irradiation Apparatus Manufacturing
10	Manufacturing	334519	Other Measuring and Controlling Device Manufacturing

10	Manufacturing	3346	Manufacturing and Reproducing Magnetic and Optical Media
10	Manufacturing	335	Electrical Equipment, Appliance, and Component Manufacturing
10	Manufacturing	3361	Motor Vehicle Manufacturing
10	Manufacturing	3362	Motor Vehicle Body and Trailer Manufacturing
10	Manufacturing	3363	Motor Vehicle Parts Manufacturing
10	Manufacturing	336411	Aircraft Manufacturing
10	Manufacturing	336412	Aircraft Engine and Engine Parts Manufacturing
10	Manufacturing	336413	Other Aircraft Parts and Auxiliary Equipment Manufacturing
10	Manufacturing	3365	Railroad Rolling Stock Manufacturing
10	Manufacturing	3366	Ship and Boat Building
10	Manufacturing	336991	Motorcycle, Bicycle, and Parts Manufacturing
10	Manufacturing	336999	All Other Transportation Equipment Manufacturing
10	Manufacturing	337	Furniture and Related Product Manufacturing
10	Manufacturing	339	Miscellaneous Manufacturing
11	Pharmaceuticals	3254	Pharmaceutical and Medicine Manufacturing
12	Defense / Military Contractor	334511	Search, Detection, Navigation, Guidance, Aeronautical, and Nautical System and Instrument Manufacturing
12	Defense / Military Contractor	336414	Guided Missile and Space Vehicle Manufacturing
12	Defense / Military Contractor	336415	Guided Missile and Space Vehicle Propulsion Unit and Propulsion Unit Parts Manufacturing
12	Defense / Military Contractor	336419	Other Guided Missile and Space Vehicle Parts and Auxiliary Equipment Manufacturing
12	Defense / Military Contractor	336992	Military Armored Vehicle, Tank, and Tank Component Manufacturing
12	Defense / Military Contractor	928110	National Security
13	Entertainment & Media	5111	Newspaper, Periodical, Book, and Directory Publishers
13	Entertainment & Media	512	Motion Picture and Sound Recording Industries
13	Entertainment & Media	515	Broadcasting (except Internet)
13	Entertainment & Media	519110	News Syndicates
13	Entertainment & Media	519120	Libraries and Archives
13	Entertainment & Media	519190	All Other Information Services
13	Entertainment & Media	71	Arts, Entertainment, and Recreation
14	Transportation / Aviation / Aerospace	481	Air Transportation
14	Transportation / Aviation / Aerospace	482	Rail Transportation
14	Transportation / Aviation / Aerospace	483	Water Transportation
14	Transportation / Aviation / Aerospace	484	Truck Transportation
14	Transportation / Aviation / Aerospace	485	Transit and Ground Passenger Transportation
14	Transportation / Aviation / Aerospace	487	Scenic and Sightseeing Transportation
14	Transportation / Aviation / Aerospace	488	Support Activities for Transportation
14	Transportation / Aviation / Aerospace	491	Postal Service
14	Transportation / Aviation / Aerospace	492	Couriers and Messengers
14	Transportation / Aviation / Aerospace	493	Warehousing and Storage
15	Public Authority / NGOs / Non-Profit	921	Executive, Legislative, and Other General Government Support
15	Public Authority / NGOs / Non-Profit	922	Justice, Public Order, and Safety Activities
15	Public Authority / NGOs / Non-Profit	923	Administration of Human Resource Programs

15	Public Authority / NGOs / Non-Profit	924	Administration of Environmental Quality Programs
15	Public Authority / NGOs / Non-Profit	925	Administration of Housing Programs, Urban Planning, and Community Development
15	Public Authority / NGOs / Non-Profit	926	Administration of Economic Programs
15	Public Authority / NGOs / Non-Profit	927	Space Research and Technology
15	Public Authority / NGOs / Non-Profit	928120	International Affairs
16	Real Estate / Property / Construction	23	Construction
16	Real Estate / Property / Construction	53	Real Estate and Rental and Leasing
17	Education	61	Educational Services
18	Mining & Primary Industries	212	Mining (except Oil and Gas)
18	Mining & Primary Industries	213113	Support Activities for Coal Mining
18	Mining & Primary Industries	213114	Support Activities for Metal Mining
18	Mining & Primary Industries	213115	Support Activities for Nonmetallic Minerals (except Fuels) Mining
19	Food & Agriculture	11	Agriculture, Forestry, Fishing and Hunting
19	Food & Agriculture	311	Food Manufacturing
19	Food & Agriculture	312	Beverage and Tobacco Product Manufacturing
20	Other	81	Other Services (except Public Administration)

CyRiM Report 2019

Nanyang Technological University Singapore

Lloyd's

Aon

MSIG

SCOR The Art & Science of Risk

TransRe We value risk.

Centre for Risk Studies
University of Cambridge Judge Business School