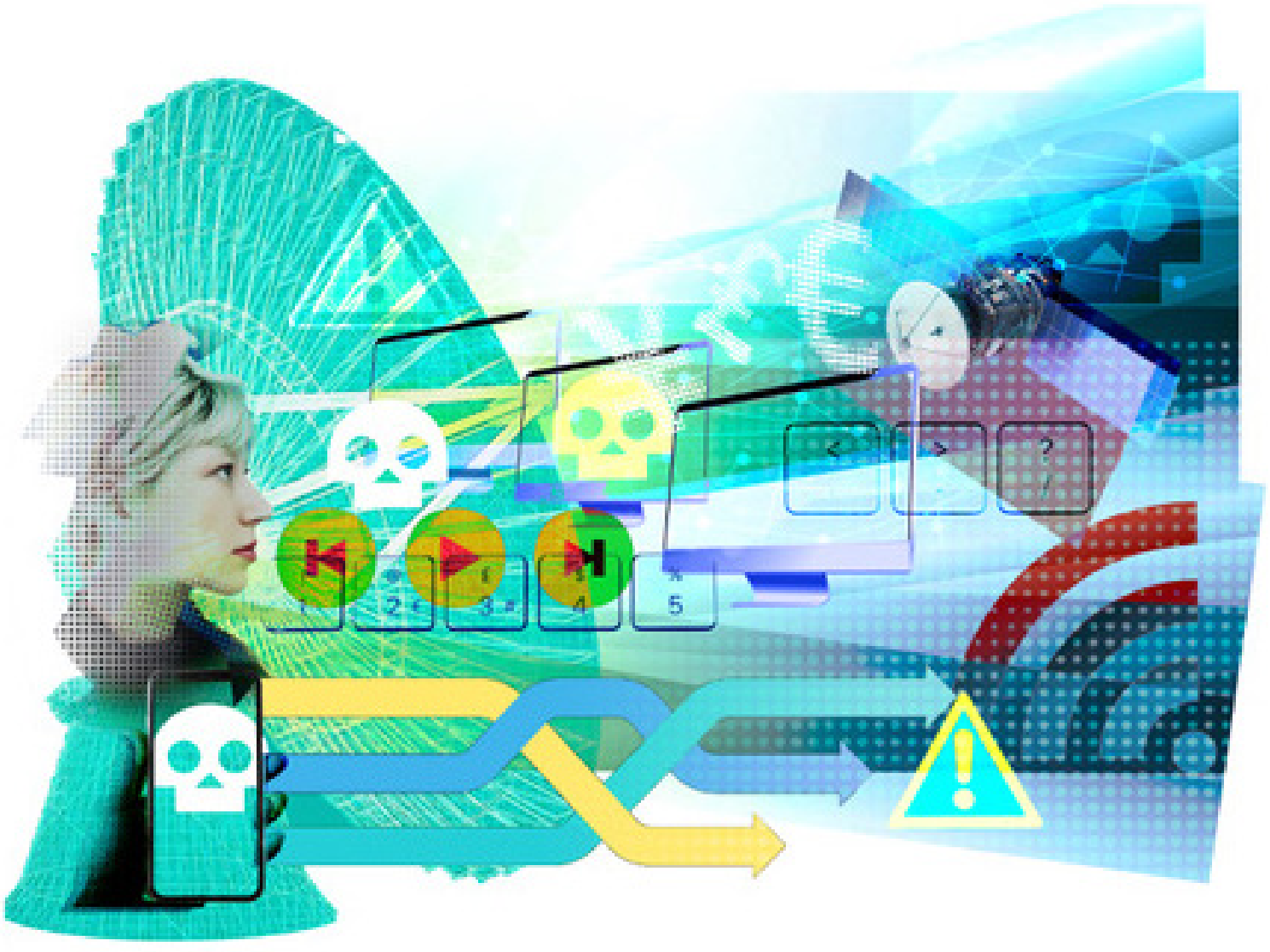
Supply Chain Risk in the Cyber Insurance Market

IUA OF LONDON
INTERNATIONAL UNDERWRITING ASSOCIATION

IUA Cyber Underwriting Group Whitepaper
in association with CyberCube
2023

CyberCube



Welcome to the International Underwriting Association's study of supply chain risk in the cyber insurance market. This paper has been produced in association with CyberCube to explore an issue that has received limited attention to date. Companies are increasingly reliant on digital support from third parties and individual cyber losses can have extensive knock-on effects across today's modern, interconnected business environment. Yet whilst war risks and other major cyber threats have been widely publicised, the importance of understanding digital supply chains has received far less attention.

It is the intention of this publication to help insurers, brokers and clients obtain a greater understanding of the exposures involved in cyber supply chain risk. An improved focus on the management of such risks will enable companies to place appropriate levels of cover capable of responding effectively to any claims.

INTRODUCTION

To manage their risks effectively in an increasingly interconnected and interdependent business environment, it is important for all organizations to gain a detailed understanding of their digital supply chain. Most organizations rely on a complex array of external vendors, technologies and suppliers to achieve their business goals. Such interconnections are a necessary part of daily operations and help them to maximize the value of their own products and services.

However, these relationships also come with inherent risks. The nature of these risks depends on each specific relationship and how they are incorporated into the organization's operations. The rise of cyber risk accumulation events has highlighted the need for cyber (re)insurers to pay attention to Single Points of Failure (SPoFs) within their insureds' digital supply chains (see Box "What is a Single Point of Failure"). Over the past few years, cyber attacks like those on SolarWinds, Microsoft Exchange, Colonial Pipeline, Kaseya and GoDaddy demonstrate why anticipating and preparing for potential risk is key to the cyber insurance industry's sustainability.

Notably, nation-state threat actors have been linked to software supply chain attacks in recent years, including NotPetya in 2017 - one of the most impactful cyber attacks of all time. The NotPetya hackers exploited several different methods to spread a combination of ransomware and wiper software to destroy data without human intervention. The original infection vector was a backdoor in M.E.Doc, an accounting software package used by almost every company in Ukraine. Companies including FedEx and Merck experienced millions of dollars worth of technology clean-up and business-disruption costs, and lost sales.

In March 2023, a software company named 3CX saw its desktop apps for Windows and macOS hacked, allowing attackers to run code on all affected devices. 3CX has over 600,000 customers and 12 million users across various industries. The attack began in 2022 when a 3CX employee installed malware via tampered third-party software called X_TRADER. The leading incident response firm Mandiant was hired by 3CX, and their report, released on April 20, stated that this was the first time they had seen a software supply chain attack leading to another software supply chain attack with the aim of attacking downstream targets.

The 3CX attack is an example of the extreme lengths to which advanced and persistent threat actors will go to achieve their objectives. The attack underscores the effectiveness of exploiting weaknesses in software supply chains - and the incorporation of this technique into threat actors' increasingly complex arsenals. The attack also highlights the imperative for enterprises to adequately monitor and secure their software supply chains on an ongoing basis.

Three Case Studies have been included in the paper to illustrate the risk.

WHAT IS A SINGLE POINT OF FAILURE?

The rise of cyber risk accumulation events has highlighted the need for cyber (re)insurers to pay attention to Single Points of Failure

As our world becomes more highly interconnected, cyber risk is an ever-growing problem. With any supply chain, digital or physical, there will be entities that specialize in providing niche services to many elements within that chain.

This specialization means that the theoretically independent supply chains of unrelated businesses may rely on a handful of providers perceived as "best-in-class" for their specialties. The net result is that an outage at one of these providers becomes a Single Point of Failure (SPoF) that could disrupt large swaths of companies that rely on them for their business operations.

While SPoFs cannot be eliminated from (re)insurers' portfolios, understanding their concentration is critical to managing risk accumulations and minimizing cyber catastrophe losses across all coverage types. Reinsurers can also distinguish which cedants are better at managing cyber risk concentration.

CyberCube's technographic data and ongoing research reveal that adoption rates for SPoF technologies have continued to increase. So when a cyber attack targets a SPoF, or uses a SPoF to reach more victims, the expected "footprint" of the attack will also increase. This increases the exposure to (re)insurers, in a similar way to how the US population moving to the coasts has increased exposure to hurricanes and earthquakes.

There are approximately 450 technologies modelled as part of CyberCube's Portfolio Manager's catastrophe model which have the highest propensity to cause a catastrophic accumulation event. There are more than 40,000 other technologies captured by SPoF Intelligence, as well as others that are not.

Exhibit 1 shows SPoF types modelled in CyberCube's Portfolio Manager Version 5 (PMv5) which make the largest contribution to modelled losses. While this is not an exhaustive list, these categories are those with the greatest potential for systemic losses across the cyber insurance industry due to their ubiquity and the heavy reliance that businesses have on such technologies. These SPoF types are further grouped into SPoF families comprising SPoF types displaying similar characteristics.

Exhibit 1

SPoF Family *& SPoF type*	Definition
Digital Service Providers	The SPoF is a provider of technology as a service; companies outsource some or all of their security responsibility to the SPoF. These scenarios can commonly result in Contingent Business Interruption (CBI) losses. If the SPoF is compromised, the SPoF will bear most of the costs of recovery.
Cloud Infrastructure	Infrastructure as a service (IaaS) and Platform as a service (PaaS).
Cloud Software	Software as a service (SaaS) - distinguished from IaaS because of the wide array of services falling into this category.
Network Services	Core web functionality including telecommunications, Internet Service Providers (ISPs), Domain Name System (DNS), certificate authorities.
Onsite Software	This is a broad category for SPoFs consisting of applications and code that sit on-premises at a company. The company bears the primary responsibility for maintaining these systems and remediating them in an incident. These scenarios can commonly result in BI losses (not CBI).
Operating Systems & Programming Languages	The SPoF is a core operating system, code library or firmware.
Operational Technology	The SPoF is an industrial control system (ICS) or supervisory control and data acquisition (SCADA) technology that controls physical operations such as power/utilities, aircraft, oil & gas production or shipping.
Money System	The SPoF facilitates the movement of money. This can include payroll systems, payment systems, and financial transaction providers. These are attractive targets for financially-motivated threat actors.
Data Aggregators	The SPoF is an aggregator of protected information for other companies by virtue of its day-to-day business. Scenarios affecting these SPoFs tend to result in widespread privacy breaches.

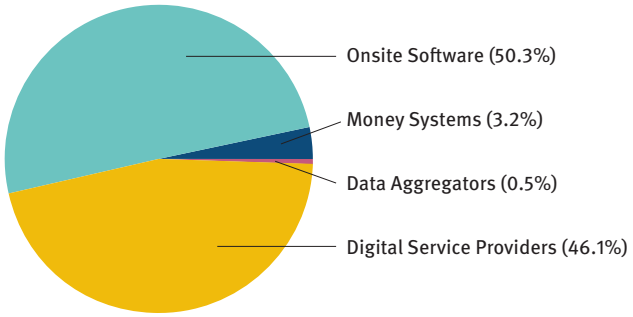
Exhibit 2 illustrates the major categories of SPoF technologies in PMv5, along with their relative contribution to 1-in-100 year industry tail risk. The largest contributor to this is onsite software such as server and endpoint operating systems (e.g. Windows, macOS, Linux, etc) and operational technology, followed by digital service providers such as cloud platform and infrastructure technologies and software-as-a service providers.

Exhibit 2: Contribution to 1:100 Tail Value at Risk – US Standalone Cyber Market

Source: CyberCube Analytics, PMv5

Critical infrastructure operators targeted

It is no longer a matter of whether, but when operators of critical infrastructure will be attacked. Such organizations should prioritize incident response planning to allow for the increasing possibility that they will face a double-extortion ransomware attack.



Reinsurers and cyber risk modelers can use CyberCube's Portfolio Manager to assess the impact on their portfolios of cyber attacks on critical infrastructure SPoF. These attacks are primarily concentrated in the Physical Damage scenario category. Users can also model losses from attacks on critical infrastructure that do not result in physical damage. For example: attacks on the banking system could lead to fraudulent payments, the downing of major internet service and cloud providers or electric utilities could result in massive unplanned downtime for organizations across a portfolio of business.

It is no longer a matter of whether, but when operators of critical infrastructure will be attacked

CASE STUDY 1: SOLARWINDS

Responsible parties: Most likely APT29 (Cozy Bear/Russian SVR)

Incident: Targeted software supply chain attack

Technical: Compromised software updates used to install backdoor access

Revealed: December 13 2020

Incident size: 18,000 SolarWinds' customers downloaded the malicious update

Countries affected: Worldwide

Who uses SolarWinds?

SolarWinds is widely considered the de-facto network management system in use within the private sector today. Following the breach, SolarWinds delivered a communication to approximately 33,000 Orion customers who were active maintenance customers during and after the malicious software updates were sent out. As well as having a large federal footprint, the company also serves major corporations in financial and payments processing sectors, industrial operations and manufacturing, along with top universities, some of the world's biggest technology companies, international airports, city governments, logistics and shipping operators.

What happened?

SolarWinds was breached by an advanced threat actor in a targeted software supply chain attack. Starting in March 2020, APT29 was able to use a compromised software update in one of SolarWinds' products to establish a backdoor into targeted systems, including the networks of FireEye, the US Treasury Department, the US Commerce Department, and DHS. The breach was revealed on December 13 2020 and, based on statements by SolarWinds, it appears that the adversary had access to targeted systems for at least nine months.

While SolarWinds was an example of a SPoF, it did not end up being a systemic event for the insurance market, as the motive was espionage and not for destruction purposes. The attacks covertly stole emails, but did not intend to destroy the data.

What are some of the key lessons learnt?

1. Supply chain attacks can have a large footprint, with a small number of targeted victims.
2. Threat actors' motivations matter greatly when determining the potential for a catastrophe.
3. Software supply chain attacks are here to stay and will become more sophisticated.

How do you model losses for this type of attack?

(Re)insurers can model losses from a software supply chain attack like SolarWinds using a mix of technology-dependency data and external network scanning techniques. Combining these datasets and techniques can help (re) insurers pinpoint the technologies in use on companies' networks. By understanding the technologies they depend on, (re)insurers can identify companies within a portfolio that are susceptible to supply chain attacks seeking to exploit those dependencies.

CyberCube's SPoF Intelligence solution offers a streamlined approach to identifying technology dependencies, at company and portfolio levels, and help (re)insurers model losses from attacks that exploit the technologies most commonly observed across their insureds' networks.

The challenges

In an increasingly interconnected environment most businesses rely on a variety of suppliers, many of which are critical to their business operation. Mapping how that supply chain integrates into an organisation's business operations is fundamental in understanding the risk exposure and actions that an organisation can take to mitigate that risk.

Insurers are reliant on clients understanding their IT infrastructure and supply chain and how any failure in the supply chain impacts their business. It also means that those third-party suppliers also need to understand their own infrastructure and supply chain to understand the risk to their clients. It is difficult for insurers to capture a client's whole exposure to supply chain as it is unlikely that they will have access to the data to assess the risk. In many cases, clients themselves have not mapped their exposure to third-party supply chains and therefore cannot share this with underwriters. Sometimes efficiency in supply chains is gained at the expense of resilience. Another factor to consider is the interconnectivity of supply chains and reliance on common technology, this can concentrate risk and aggregate losses.

There is also a resiliency question around, for example, manufacturing when a cyberattack disrupts cyber operations of third-party suppliers themselves rather than using them as a vector to access the insured. Subsequent nonavailability of third-party suppliers output will then impact the operational capability of the insured. This makes this more complex not only from an insured's third-party supplier management strategy or procedure perspective, but also in that it increases the threat surface area significantly.

The Pandemic highlighted significant challenges in global supply chains and had the effect of temporarily halting the flow of some raw materials and finished goods. As a result, many manufacturing industries were significantly disrupted. This exposed the vulnerability in supply chains which apply not only to cyber, but are also inherent in all supply chains that organisations rely on. A prime example of disrupted supply chains during the Pandemic was the impact on the manufacturing of semiconductor chips in Taiwan, where it is generally agreed that 60% of the world's semiconductors are produced. This impacted various industries including car manufacturers and consumer electronics, and in particular those firms that did not have sufficient reserve stocks to continue their operations.

The nature of cyber loss can mean that if an insured sustains a business interruption loss due to a supply chain attack, causation must be established. More often than not, there is no physical damage to the insured's property, so the insured will need to allow the insurer (via an appointed relevant investigator) to access their IT infrastructure and prove the covered event occurred. Should the loss have occurred via a third party through the insured's supply chain, this will need to be established and the third party involved should provide

In an increasingly interconnected environment most businesses rely on a variety of suppliers, many of which are critical to their business operation.

details of the incident to the insured. The third party could then be potentially liable for any losses that arise, but this will be governed by the terms of the contract the insured has entered into with the third-party supplier.

There has been limited success in recovering an insured's loss for the part of the supply chain at fault (subrogation) and many contracts with third-party suppliers will limit or exclude losses of this nature. There are limited exceptions in niche areas of the market, but on the whole, this has not proven to be a reliable method of recovering losses and recovery via subrogation tending to be minimal.

Another challenge that the IUA Cyber Underwriting Group identified is the availability of IT forensic firms in the event of a widespread loss and whether there would be sufficient resource to assist all those that have been affected. Again, this is problematic to manage, not only for the industry but for clients more generally.

One approach that has been seen in the market is to limit the exposure to named critical suppliers, another is to impose a general limit. There may be other approaches adopted by the industry but regardless of the exposure, this aspect remains very difficult to manage.

CASE STUDY 2: DROPBOX

Responsible parties: Unidentified

Incident: Data breach

Technical: Gained access to a GitHub account using employee credentials obtained in a phishing attack

Revealed: 1 November 2022

Incident size: 130 code repositories copied

What happened?

On November 1, 2022, San Francisco-based Dropbox announced that it had fallen victim to a phishing campaign resulting in unauthorized access to 130 source code repositories on GitHub. The attack mainly affected third-party libraries used by Dropbox, with core apps spared. Along with the leaked source code, the attack also gave the attacker access to thousands of employee names and email addresses, as well as to sales leads and vendors' information.

The attack began in early October when employees received phishing emails posing as having been sent by CircleCI, a software development tool used by Dropbox. The emails, which had bypassed spam-detection filters, prompted employees to click on what was purportedly a link to CircleCI's login page and enter their GitHub credentials.

This allowed the attacker to gain access to Dropbox's repositories and hence to sensitive information for possible use in further intrusions.

What are some of the key lessons learnt?

1. Even the biggest SPoFs are vulnerable (Dropbox has 700 million users), highlighting the need to model attacks on these targets.
2. The data stolen in the Dropbox breach could have led to the creation of sophisticated phishing lures aimed at Dropbox customers.
3. The attack reminds us that the human element of cyber security remains unsolved, with phishing yet again proving itself effective.

How do you model losses for this type of attack?

CyberCube has an accumulation path based on a major online data storage firm and all data they store on behalf of customers being encrypted by ransomware, causing organizations around the globe to lose access to their data for several days while the firm responds and recovers.

CyberCube models a ransomware attack on a SPoF like Dropbox, in which data is also stolen. The use of ransomware would cause unplanned downtime for Dropbox and its customers in addition to losses from data exfiltration.

Due diligence/Best practice

Clients that have a good idea of what their supply chain looks like and can demonstrate that they have a good governance framework to manage their supply chain are likely to be able to source cover for their needs more easily than those clients that cannot. Credit checks and financial viability analyses of suppliers and an understanding of the contribution of each vendor in the supply chain to a client's own business will allow for proper operation and also enable clients to map their reliance on the vendor landscape as a whole. Undertaking a business impact analysis of the failure of any of those vendors, what that looks like in monetary terms can highlight areas to introduce mitigation strategies that will build resilience and redundancy measures. Brokers preparing insurance clients to be able to provide that information will greatly assist in sourcing cyber insurance cover.

There are vendors that can offer to interrogate a client's supply chain as to their cyber risk maturity and can additionally monitor this over time but often that will include obtaining agreement of the vendors in the supply chain. It is important to note that if there is not ongoing monitoring, information provided to source cyber insurance represents a single point in time and is essentially an attestation that a component of an insured's framework is compliant at a certain date – digital environments change, need maintenance, updating and patching. Generally, a cyber insurance policy will provide cover for a year and the information presented when sourcing a policy will need to be maintained for the life of the policy.

Cybersecurity awareness training helps to educate an organisation's employees about the need for security measures, raises awareness of potential threats and helps to reduce the risks associated with cyber attacks.

A summary of key underwriting considerations:

- Has the organisation developed a response/ Business Continuity Plan from a cyber peril exposure?
- Testing of the cyber supply chain.
- Has the organisation conducted a review of their supply chain exposure to a cyber attack?
- Has the organisation reviewed their suppliers' Business Continuity Plans/response to a cyber attack?
- Does the organisation and its suppliers deliver cybersecurity awareness training to its employees?
- Identifying suppliers that use the same software (an accumulation of potential risk).
- Are control systems and/or manufacturing systems isolated from the external systems?
- Does the organisation rely on one supplier to meet their needs or are there alternative suppliers?
- Do contracts with suppliers include service-level agreements and are there contingencies included where the supplier is unable to provide the service?
- How long would the interruption suffered by the supplier be - days, hours, weeks or months?

CASE STUDY 3: COLONIAL PIPELINE

Responsible parties: FBI attributes attack to the DarkSide gang

Incident: Ransomware attack

Technical: A targeted attack on Colonial Pipeline's IT system causes pre-emptive OT shutdown

Revealed: Saturday May 7 2021

Incident size: 100GB of technical data and lost revenue due to downtime. Additional losses included breach remediation, recovery, ransom payment ($5M), and reputational losses

Countries affected: United States, particularly the Eastern Seaboard's access to fuel

What happened?

The attackers (DarkSide) inadvertently took down 5,500 miles of critical US oil pipeline infrastructure. DarkSide, a financially motivated ransomware-as-a-service (RaaS) gang, apologized for the "social consequences" of the attack.

On Saturday, May 15, after one week of downtime and a $5 million ransom payment, Colonial Pipeline said its systems were back up and running at full capacity. However, before Colonial Pipeline had (even partially) restored its systems, thousands of gas stations ran out of gas, as panic buyers rushed to fill up. State governors in Florida, Georgia, North Carolina, and Virginia implemented states of emergency due to gasoline shortages. Gasoline suppliers had to cut production to avoid excess product on the supply end.

What are some of the key lessons learnt?

1. The double-extortion ransomware attack on Colonial Pipeline once again brings enterprise ransomware into the spotlight for cyber underwriters and cyber risk aggregation modellers.
2. The attack underscores how critical it is for underwriters to assess basic cyber hygiene along with threat-specific risks such as ransomware for all organizations, regardless of size or industry, but especially for critical infrastructure.
3. The attack also calls attention to the risk of widespread contingent business interruption (CBI) as a result of attacks. The attack is an example of accumulation risk due to cyber attacks on SPoF technologies and companies.

How do you model losses for this type of attack?

CyberCube's Portfolio Manager models catastrophic cyber aggregation events. Scenario 6 models malware targeting security flaws in the programmable logic controllers (PLCs) used extensively in the control systems of mobile offshore drilling units (MODUs) resulting in property damage and business interruption, with disruption to the US oil supply. In this accumulation path: Spear phishing attack on a SPoF results in malware deployment causing damage to multiple MODU units, life liability, and pollution issues. Owners of MODUs experience downstream impacts and the offshore drilling industry experiences disruption.

Business impact analysis/methodology

The working group considered how supply chain exposure could be made easier to manage and it was suggested that raising awareness of the exposure with clients and brokers could be a useful first step, in addition to gaining understanding as to what was meant by supply chain. Encouraging more clients to undertake risk assessments will assist in understanding the exposure to a particular client and the wider exposure in general. There are companies offering calculators/models in respect of supply chain risk but these are in their infancy and would currently be of limited use.

A wider understanding of supply chain risk by specific sector and/or business size, in addition to the frequency and reliance on particular systems, would assist all parties to understand the exposure in much more detail. It is useful for the insurance industry to understand how a potential insured has taken any analysis and factored it into their own resiliency and redundancy.

As demonstrated by the issues with semiconductor chip manufacture by Taiwan during the Pandemic (see the section 'The challenges'), should an organisation have a single supplier with limited backup stock or raw materials, this can result in a complete halt to business operations. Organisations that plan contingencies in respect of their main suppliers will be far more resilient than those competitors that do not.

Given the limited take-up of cyber insurance when compared to other classes of insurance, there is only a small amount of data available to the insurance industry to build a comprehensive picture.

Understanding cyber data

In January 2023, the Bank of England published the results of the Prudential Regulatory Authority's Insurance Stress Test 2022. It noted that "In light of the growing adoption of vendor models, we encourage boards to understand the limitations and lack of convergence in existing cyber catastrophe modelling, and to ensure that they are satisfied with any measures taken to mitigate shortcomings in current approaches."

Cyber models do vary in their approach, which is to be expected with an evolving risk. Much of the "lack of convergence" can be understood by taking a closer look. It's important for regulators examining cyber model results to understand key assumptions made in the model, as well as assumptions made by the company reporting the model results. These are not always the same; many insurers adjust model settings to fit their organization's view of risk.

Regulators would be well-positioned to ask clarifying questions such as:

- Did you use a vendor model? If so, which one?
- Did you make deviations from the vendor's default settings? If so, how and why?
- If you did not use a vendor model, what approach did you use? Why?
- How does your model estimate frequency? To what extent is it based on historical losses versus expert judgment? To what extent is it informed by the current threat landscape?
- Which SPoFs do you see presenting the greatest loss potential?
- For cloud risk, were malicious attacks explicitly contemplated? Were accidental outages included?

The PRA paper focuses on insurers' reported differences in frequency estimates. CyberCube regards it as important not only to consider frequency but to also understand the financial impact to insurers given that the event in question does occur. If an insurer would be materially affected, this should be the first concern. Additional insights can be gained by looking specifically at the event characteristics at certain points in the tail such as the 1 in 100 probable maximum loss. Questions to consider include:

- Which cyber events contribute at this level?
- What portion of insureds are affected and why? Are any segments particularly vulnerable?
- What level of losses are reflected on individual claims? How do these compare against the actual claims activity of the insurer? Are the differences understood?

It is important for a company to have a thorough understanding of its external relationships so that it can factor them into a comprehensive risk management plan. Similarly, any

It is important for a company to have a thorough understanding of its external relationships so that it can factor them into a comprehensive risk management plan

(re)insurer or broker attempting to understand a client's risk needs to incorporate the inherited risk of these external relationships into its assessments.

It is important to comprehend, not only the presence or absence of a technological relationship between two organizations, but also the level of confidence that can be attributed to such a claim, and the degree to which organizations are reliant on these vendors. Such a metric has the potential to allow the creation of more accurate risk management policies by correctly discounting low-confidence data findings and prioritizing high-confidence findings.

However, data that captures relationships is often incomplete and lacks the rigorous validation required for building a reliable risk management plan. This process often starts with examining a variety of digital artifacts relating to an organization, such as technology web fingerprints, regulatory filings, and automated text analysis, and then employs a variety of heuristics to infer technological dependencies on the basis of those measurements.

Conclusion

Supply chain management is a complex and little understood topic. Understanding what an organisation's supply chain looks like is fundamentally important in order to assess the impacts of any supply chain disruption. Snapshots of supply chain risk taken at a particular point in time do not consider how risks may evolve through a firm's financial planning cycle; therefore ongoing oversight and governance are critical. This equally applies to the lifetime of any insurance contract that an organisation may purchase to transfer some of the risk.

Those organisations and their brokers that can articulate clearly what their supply chain risk is and measures adopted to mitigate that risk will be in a better position to source cyber insurance cover at the levels required. Overall, any organisation that has a good understanding of their supply chain risk and how it may effect their business should that supply chain be disrupted will improve their operational resilience and reduce threats to the continuity of trade.

APPENDIX

About the IUA

The International Underwriting Association of London (IUA) is the representative body for companies in London providing international and wholesale insurance and reinsurance coverage. Its mission is to secure an optimal trading environment for London insurance companies.

The IUA's Cyber Underwriting Group was established in 2014 to provide a forum for underwriters offering specialist cyber risk coverage in the London company market. The Committee considers cyber from the context of standalone cyber cover and considers issues relating to the underwriting and handling of claims in the London market (irrespective of the territorial extent of the cover) arising from "cyber" risk and insurance, both first and third-party.

About CyberCube

CyberCube delivers the world's leading cyber risk analytics for the insurance industry. With best-in-class data access and advanced multi-disciplinary analytics, the company's cloud-based platform helps insurance organizations quantify cyber risk to facilitate placing insurance, underwriting cyber risk and managing cyber risk aggregation. CyberCube's enterprise intelligence layer provides insights on millions of companies globally and includes modeling on thousands of points of technology failure.

The CyberCube platform was established in 2015 within Symantec and now operates as a standalone company exclusively focused on the insurance industry, with access to an unparalleled ecosystem of data partners. It is backed by Morgan Stanley Tactical Value, Forgepoint Capital, HSCM Bermuda, MTech Capital, individuals from Stone Point Capital and Scott G. Stephenson. For more information, please visit www.cybcube.com or email info@cybcube.com.

CyberCube Contributors:

Jon Laux, VP of Analytics

Manish Karir, VP of Data

William Altman, Cyber Threat Intelligence Principal

Yvette Essen, Head of Content, Communications & Creative

International Underwriting Association Ltd
London Underwriting Centre, 1 Minster Court,
Mincing Lane, London EC3R 7AA
tel +44 (0)20 7617 4444
email info@iua.co.uk **web www.iua.co.uk**