CyberCube

ACCURATELY ASSESSING SILENT EXPOSURE: A STEP TOWARDS STRENGTHENING THE CYBER MARKET'S DEVELOPMENT

DECEMBER 2019

Author
Ashwin Kashyap, Co-founder, Head of Product & Analytics

Editorial Manager
Yvette Essen, Head of Content & Communications

Introduction

Against a backdrop of increasing interconnectivity, the need to accurately price cyber risks, understand gross and net exposures, and gain deeper insight to steer underwriting towards better exposure controls and profitability is paramount.

This is particularly challenging when exposures have in many cases changed from tangible physical risks to intangible digital exposures. As a result, cyber risks and exposures need to be accurately factored into the pricing of existing standard property and casualty (P&C) policies, especially if there is a desire to cover them in existing portfolios. Companies need to balance their risk management and competitive positions with the need to charge appropriately for risks.

Traditional approaches to risk accumulation management have not proactively considered cyber risks across multiple lines of business. As a result, there may be unknown potential for risk accumulation within portfolios for P&C risks. In recent months, the (re)insurance industry has taken some positive steps to address the issues raised by non-affirmative cyber, but more effort is needed in relation to cyber risk management.

The connected exposures and premiums at risk across all P&C lines of business that could be impacted by cyber is an order of magnitude higher than stand alone affirmative cyber premiums, which market participants have estimated to be around $5.5 billion globally.

Where Does Coverage Ambiguity Lie?

Ambiguity in (re)insurance contracts can cause direct exposures in a policy or even potential accumulation across policies where the cyber peril is neither explicitly included nor explicitly excluded. This has the potential to create ambiguity in interpretation as to whether a given loss event (whether physical or non-physical), originated by a cyber-related peril is covered by a standard policy. Many of these policies were developed in a pre-internet era which did not contemplate digital risks. This is known as non-affirmative cyber (or silent cyber) risk. In today's interconnected and interdependent business environment, this leads to concern for policyholders surrounding non-physical perils such as a network/system failure that causes disruption to business continuity and profitability. By way of contrast, affirmative cyber cover refers to insurance policies where the peril is defined and clearly set out within a policy document.

What Is the Impact?

If the issue of silent cyber is unresolved, this will have a detrimental impact for the development of both the affirmative cyber market as well as hinder the P&C market.

Lack of clarity creates ambiguity for the insurance buyer as well as results in unknown exposures for insurers and reinsurers.

Legal precedent when it comes to silent cyber risk is largely untested in the courts. Leaving the legal system to decide whether damage arising from a cyber event is able to address evolving exposures will be a challenging experience for the insurance industry and a lucrative line of business for lawyers. It will be interesting to observe how the market reacts to future losses and court decisions.

Supervisors Help Fuel The Need for Greater Clarity

In most global companies, cyber risk is a board level concern with many chief executive officers (CEOs) placing this threat high on the list of the biggest existential threats. The results of a survey published in January 2019 by the UK insurance regulator, the Prudential Regulation Authority (PRA), highlighted how silent cyber is featuring on CEOs' radars.

Supervisors, such as the PRA, have played an important role in encouraging insurers to take an active role in measuring and managing silent cyber risk. Anna Sweeney, the PRA's Director of Insurance Supervision, detailed the survey results in a letter to insurance CEOs. She stated that a number of traditional lines of business have considerable exposure to non-affirmative cyber risk and cited concerns that certain classes, including casualty and motor, have the largest non-affirmative exposure (see Lines of Business Where Silent Cyber is Prevalent).

In July 2019, Lloyd's mandated all of its syndicates will be subject to a January 1, 2020 deadline whereby they must start to address silent cyber in contracts across all first-party property damage lines of business that they deal in. In a Market Bulletin (Y5258), the (re)insurance market stated that it will require insurers to explicitly state whether cyber coverages are included or not. Furthermore, acting PRA Director, Insurance Supervision, Gareth Truran has highlighted how underwriting strategies and emerging risk trends are being assimilated into exposure management practices as areas of upcoming PRA focus. In November 2019, he encouraged the industry to develop more robust approaches to assess man-made catastrophe risks. He reiterated how the PRA has asked firms to develop action plans to address residual "silent" or "non-affirmative" cyber exposures, in the expectation that companies which have not yet acted will be able to show "demonstrable progress" in the months ahead.

Other stakeholders, such as ratings agencies and investors, are also seeking greater clarity. They are requiring companies to proactively evaluate and measure their cyber risk accumulation exposures across the range of P&C classes of business.

Lines of Business Where Silent Cyber is Most Prevalent

One of the biggest challenges facing the insurance industry is in helping insurers understand where non-affirmative exposure exists, and clarify their coverage positions clearly. Lloyd's has stipulated that managing agents must be explicit as to whether cyber is included or excluded within property risks in January 2020 (including coverholders). Liability and reinsurance policies will follow by 2021.

The PRA has stated concerns about a number of traditional lines of business that have considerable exposure to non-affirmative cyber risk, including casualty, financial, motor and accident & health (A&H) lines. These example loss scenarios illustrate the potential for cyber attack to reach every part of modern society, and consequently impact a very wide range of insurance classes, including:

- a cyber attack can directly impact the share price of a publicly listed company, especially when it undermines trust in corporate governance
- a denial of service attack which prevents logistics systems operating in transportation companies
- a ransomware attack which shuts down operations of shipping companies
- manipulation of operational technology, leading to physical damage and bodily injury, for example against industrial control systems in the manufacturing sector
- disruptive attack against critical national infrastructure, resulting in system-wide outage

Fears of endemic losses due to Business Interruption (BI) are fuelling the need for clarity as to how contracts would respond and whether the entire limit is exposed to cyber risk. If BI classes are exposed, this could have ramifications on pricing and risk management.

The 2017 NotPetya attack on a widely-used Ukrainian tax software spread rapidly using a combination of existing malware, causing systems to be shut down due to a malicious code. This illustrates the potential for business interruption losses to manifest across a wide range of industries and classes of insurance. Companies impacted most were those who had operations connected to those in the Ukraine.

Estimates of the economic impact range from $4 billion to over $8 billion and many household company names were impacted, including Maersk, Fedex, and Merck.

Maersk alone has acknowledged a $300 million cost for the attack. The consensus is that genesis of the attack was the Russian government which has led to increased concerns around how to defend against hostile cyber activity.

Ever since the NotPetya cyber incident in 2017, and also the WannaCry attack in the same year, it has become evident that cyber threat actors can seriously disrupt or even halt business operations.

Property BI losses have regional boundaries, whereas cyber attacks have the potential to trigger simultaneous interruptions globally.

In addition to BI, other traditional lines of business have the potential to create cyber exposures. These could include: physical damage, extortion payments and extra expense from ransomware, and/or liability from general liability policies.

Energy lines of business are perceived to have low non-affirmative exposure, mainly due to the application of exclusion CL380 - a widely-used exclusion across marine lines. This exclusion has been hotly debated in its application in the market and relevance today.

Industry Response to Date

Traditional insurance products were developed before cyber risk become a meaningful concern for (re)insurers. As conventional insurance policies were not designed to include cyber as a potential risk, they did not specifically reference digital perils (either proactively incorporating or excluding) as these were not actively considered at the time of underwriting. Recently developed insurance products are more explicit as to whether cyber risk is covered.

As the cyber insurance market matures, many insurers are taking active measures to bring together their cyber exposures explicitly. One well-known strategy here is to consolidate all cyber exposures in a standalone line of business that can then be managed more effectively. Insurers are reviewing policy wordings, engaging with experts on legal matters and developing products to determine whether there is exposure resulting from cyber-related events.

Insurers face challenges if they are held responsible for cyber-related claims as a result of “ambiguous” policy wordings in standard commercial products, such as BI covers.

Some insurers are moving to address this grey area with plans to affirm whether their commercial policies cover or exclude cyber risks.When insurance carriers are clearly able to outline what cyber risks are insured, they will benefit by being able to improve understanding and management of their exposure. Balancing the transition to improved clarity around cyber exposures is imperative, as is remaining competitive in a landscape where business continuity is vital to productivity and brand reputation.

"Balancing the transition to improved clarity around cyber exposures is imperative, as is remaining competitive in a landscape where business continuity is vital to productivity and brand reputation"

One approach by carriers relating to silent cyber is to exclude this exposure. However, insurers may not want to disrupt the coverage in place for their clients in any meaningful way. Managing this change whilst maintaining trust and a competitive position is consequently very difficult.

Meanwhile, brokers are advising their clients on the best cyber resilience and risk management practices based on learnings from the market. They have also identified certain classes of businesses to have a higher probability of being exposed to silent cyber such as product liability, director's and officer's (D&O), kidnap & ransom (K&R), property and crime.

Increasingly, brokers use risk models to manage non-affirmative exposures as well as plan imagined scenario loss events to understand how these perils may manifest in different types of policies. They are working with model developers like CyberCube to enhance the suite of capabilities available to help with the measurement of cyber risk in these lines of business.

Reinsurers Motivated to Find Solutions

Reinsurance risk accumulation is a real concern. Long-tail casualty has been prone to systemic risk and shockwaves that can collapse markets. The asbestos crisis that almost brought Lloyd's to its knees in the 1990's is a case in point. More recently, the opioid crisis that is currently engulfing the US has the potential to deliver a devastating blow to insurance balance sheets and many well-seasoned market experts have similar forebodings when it comes to the silent cyber threat.

When examining all P&C reinsurance lines of business, treaties are exposed to various cedant contracts - many of which may be silent on whether they respond to cyber loss activity.The cumulative effect of this can result in unknown exposures in certain lines of business for reinsurers.

"Coverage in primary insurance contracts should mirror that provided by reinsurance treaties to avoid gaps"

Threat actors that take advantage of interdependencies across digital and physical supply chains, add fuel to the fire for reinsurers. Extreme events with high uncertainty and limited (or no) precedent imperil all industries, markets and companies.

It is important for (re)insurers to develop a clear understanding of (re)insurance contracts and what level of uncertainty exists in whether an insurance contract explicitly covers cyber losses. Once this is understood, models can be run against these exposures to estimate the likelihood and severity of losses. Not all types of events would result in claims so it is equally fundamental to configure models to ensure that only applicable events are considered.

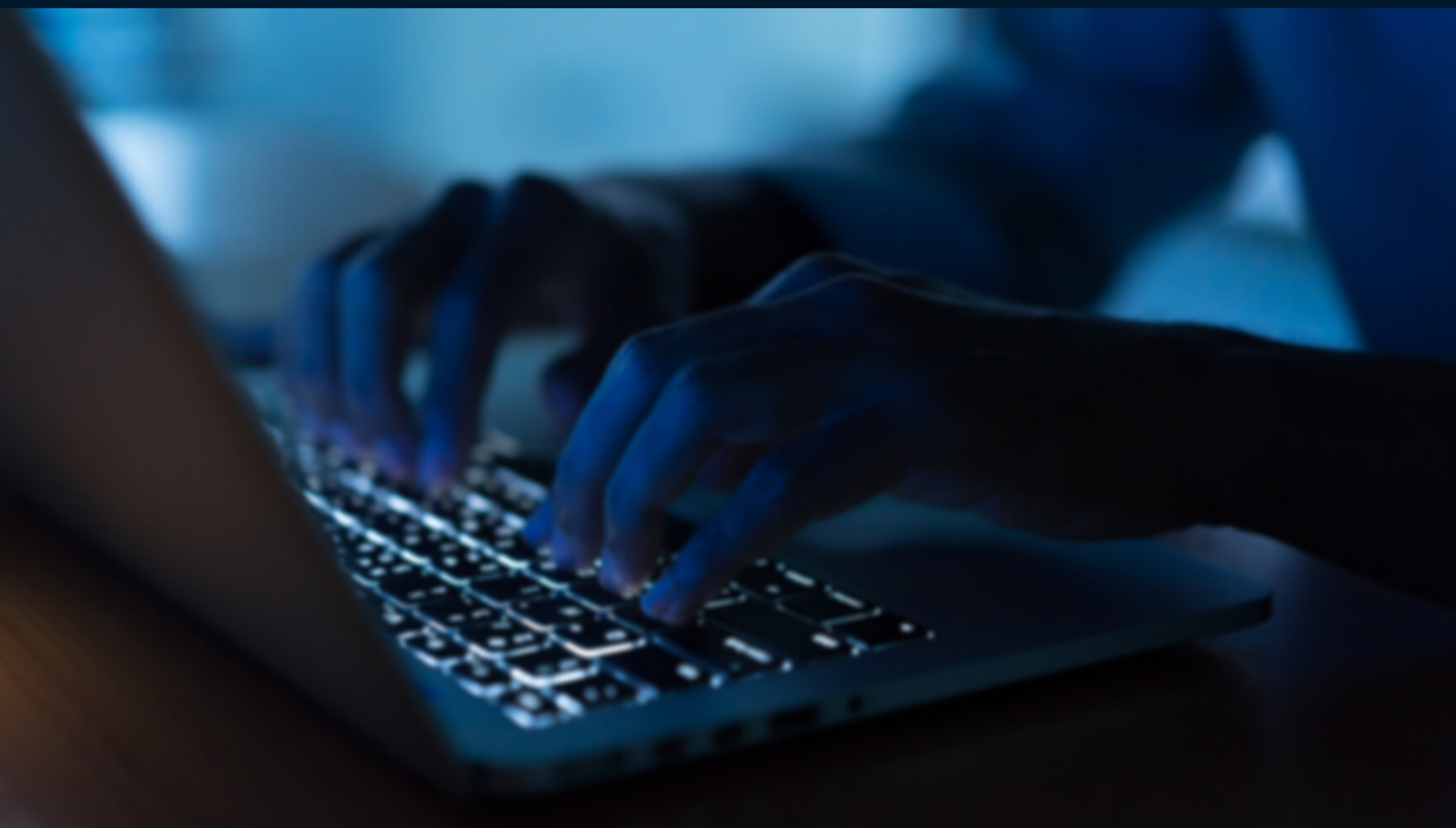
Reinsurers are encouraging their cedants to eliminate ambiguity in their contracts. Furthermore, reinsurance contracts in many cases explicitly exclude cyber risk in treaties related to other lines of business. One critical consequence of this is that coverage in primary insurance contracts should mirror that provided by reinsurance treaties to avoid gaps in coverage. To address cases where reinsurance contracts are silent on cyber risk, a conservative position would be to assume that the treaty would likely pay out in the case of a cyber attack.

The Use of Models for Silent Cyber

The rapid growth of cyber insurance creates challenges for claims professionals and carriers seeking to set loss reserves and forecast capital requirements for a product that has limited structured data or loss history (with the exception of a small number of larger market players) attached with it. Determining cyber loss reserves are likely to draw on other lines of business (historically cyber has been part of financial/specialty lines - D&O/E&O), but it is very hard to allocate definitive loss reserves for the development profile of these incidents. For insurers, scenario-based modelling is the route forward.

Models can be helpful in running ‘what-if’ analyses on exposures to help determine whether the risk in any line of business is substantial and warrants timely action. Being able to measure this risk enables it to be managed more effectively.

Silent cyber models have traditionally been restricted to property lines of business. CyberCube’s approach is to make it applicable across all lines to enable a broader view across the spectrum of P&C risks. This includes lines of business such as aviation, marine, product liability, offshore energy, and kidnap and ransom.



A key area to focus on is multi-line accumulation, as a systemic cyber event might result in losses (for example) under D&O and product liability covers.

More and more underwriters are working with risk modellers to understand loss potential and outcomes. CyberCube has developed a variety of features on our market-leading cyber risk modelling platform to enable our clients to model cyber-related perils as they manifest across all lines of business. We consult with our clients to determine best practices around the usage of our model based on key exposures in particular lines of business. For example, the model addresses coverages within Technology E&O policies from the scenarios that have already been developed.

The CyberCube platform provides ways to help understand these exposures through mapping cyber perils to P&C lines of business and modelling the results of our carefully designed scenarios in a probabilistic manner.

Author:

Ashwin KASHYAP, Co-founder, Head of Product & Analytics

Editorial Content:

Yvette ESSEN, Head of Content & Communications at CyberCube