KOVRR
Cyber Risk Modeling

Cyber Risk: from Peril to Product

A New Approach for Managing Silent Cyber Risk

MARCH 2020

KOVRR
Cyber Risk Modeling

Cyber Risk: from Peril to Product

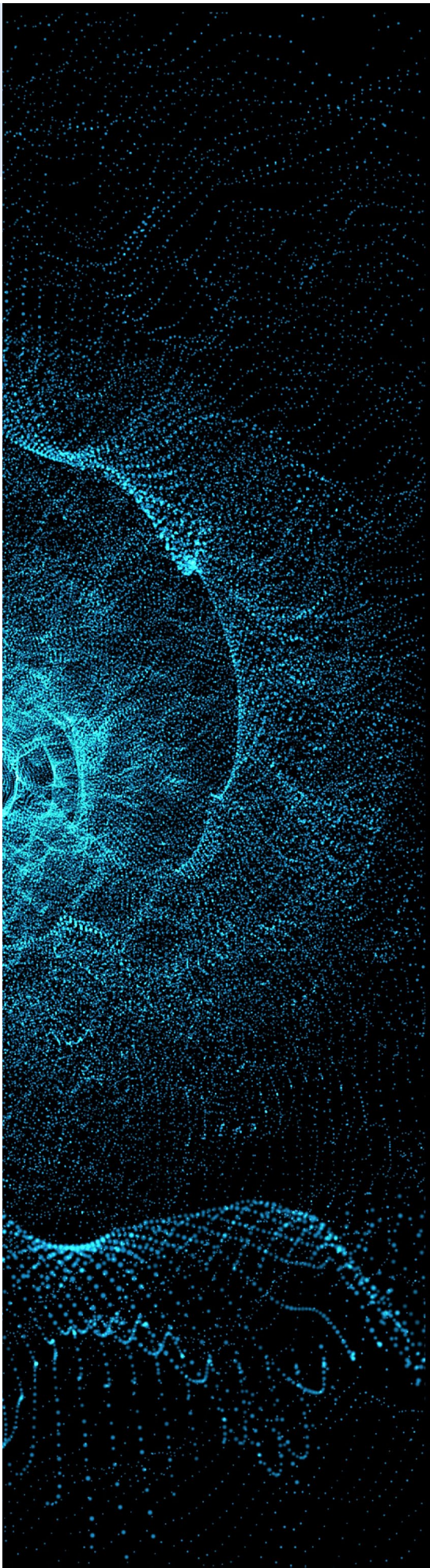
A New Approach for Managing Silent Cyber Risk

Cyber is a multifaceted peril that is both a threat and an opportunity for the insurance industry: an opportunity because of the ever-evolving needs of coverage for businesses of any size, and a threat because of the systemic risk arising from its potential for overlap with other lines of business. Silent cyber refers to covered losses triggered by cyber events in P&C policies that were not specifically designed to cover cyber risk. Affirmative cyber refers to coverages specifically provided to protect policyholders against cyber events and presents a premium growth opportunity for insurance companies. As exposures to cyber continue to grow, insurance companies need tools to quantify the impact on allocated capital for cyber risk, regardless of whether the risk is silent or affirmative.

With some estimates for accumulation across commercial lines running in the hundreds of billions, exposure managers are under pressure to more accurately estimate the potential impact of cyber events to ensure appropriate capital is held for this risk and enable decision makers, investors and regulators to quantify financial returns on a risk adjusted basis. Additionally, they are being forced to provide more transparency into methods used for measuring and controlling cyber accumulations. With various stakeholders and types of practitioners involved, the topic of cyber risk often presents seemingly conflicting priorities around managing capital at risk, estimating potential losses in existing lines of business, and finding new ways to market, through pricing new cyber specific business.

Cyber events across different lines of business share a common trait. The key is to build tools capable of estimating realistic losses for both silent and affirmative cyber based on these shared traits. The focus of cyber risk for insurers should be gaining unique insights into events that truly matter - events capable of generating equity depleting losses. Measuring the impact of cyber events on capital is a three step process: identify, quantify and manage.

Lately, the insurance industry seeks to consolidate most cyber risk into one dedicated line of business by implementing exclusion clauses in existing policies and inviting policy holders to “buy back” coverage. Several different wordings for such exclusions and endorsements have been introduced to the market. While intending to clearly define the scope of a cyber event and the coverage provided, the introduction of some of these clauses has produced unintended consequences. One example of this would be coverage for damage to a server due to flooding. In this example, the common expectation would be for the physical damage to the server as well as recovery of the data to be covered under flood insurance, however, the latest trend suggests data recovery might be excluded, as it relates to ‘data’, leaving a gap in coverage for property which some sources consider excessive.



Silent and Affirmative

The issue with silent cyber, as with any circumstance presenting unexpected claims activity, is ensuring the premium charged is commensurate with the level of risk, usually referred to as pricing adequacy. Both cyber exposure and the potential impact of losses triggered by cyber perils continues to trend upwards annually. Unexpected claims lead to unexpectedly high loss ratios which clearly erode profits but can also lead to significant damage to an insurer's financial stability.

Insurance companies protect their balance sheets by purchasing reinsurance, but reinsurers face similar issues, they are also vulnerable to silent cyber. Therefore, insurers face the prospect of being denied recoveries from cyber losses and reinsurers are stepping up demands for clarity of coverage. Efforts to resolve the situation have taken two complementary directions: a conscious attempt to price for cyber risk and the introduction of increasingly restrictive exclusion clauses.

The Status of Cyber Exclusions

Cyber exclusions have been a staple of the insurance business since the late 1990s, when the "millennium bug" (also referred to as Y2K) made computer systems unable to distinguish between the 1900s and the 2000s. Amid exaggerated reports of possible impending disasters, insurers introduced a Y2K exclusion on existing policies and offered specific Y2K coverage on the side. Since then, several different cyber exclusions have been developed, the most common of which is CL380* introduced in 2003. Widely considered to be a broad exclusion, the CL380 remains silent for a wide range of events, including in some circumstances a large service provider outage. The main issue with CL380 is when challenged in court it may prove to be less restrictive than originally intended. For example, any malicious attack is supposed to be excluded, but if the attack didn't intend to cause harm directly to the insured, a court might decide the claim to be valid.

Regulatory authorities have started to become more involved, with the specific aim of protecting the market, because a cyber catastrophe has the potential to cause insolvency and widespread economic damage. Most recently, the Prudential Regulation Authority expressed concerns about potential accumulations of cyber losses in the market and called for all regulated entities to step up their efforts to quantify and manage cyber risk. Lloyd's introduced a phased approach in January 2020, specifying all cyber incidents, whether malicious or non-malicious should be covered under affirmative cyber policies or excluded altogether. Two new property exclusion clauses were released, LMA5400 and LMA5401, the latter of which goes as far as excluding data recovery after a flood.

* http://www.legislation.gov.uk/eur/2009/392/annex/ii/appendix/a/division/2/adopted

Cyber Risk Modeling

Exposure managers are well versed in looking at natural hazards and quantifying potential accumulations using several different tools. Catastrophe models are used throughout the risk transfer chain, from insurers to capital markets. It is therefore only natural for exposure managers to adapt existing tools and processes for cyber. Their main priority is to deploy capital on cyber risk purposefully and efficiently. Models need to meet this primary objective first, to enable the market to quantify the impact of cyber losses on capital, set risk appetites and ultimately enable risk transfer where possible.

The Role of Cyber Expertise

Several different modeling frameworks for cyber are currently being offered to the insurance market. Unlike natural hazard frameworks, frameworks for cyber risk can differ in scope but also in purpose, making it difficult for exposure managers to compare vendor models and select the right tool. Model vendors need to be very clear about the risk traits they capture in order to explain how their models portray both the risk landscape and the way the landscape develops.

A valid and dependable cyber risk modeling framework should take into consideration and encompass the following concepts and their dependencies:

- Vulnerabilities and exposures*: either a specific issue with a technology or a failure of a third party service provider product
- Threat actor: someone capable of exploiting one or more vulnerabilities
- Campaign: an attack or series of attacks by a threat actor leveraging specific vulnerabilities, tools and techniques

Understanding vulnerabilities and exposures is very important but not enough, because a vulnerability on its own cannot produce a loss. At the same time, focusing too much attention on threat actors can be distracting. At Kovrr we look at the actions of threat actors, by studying real time exploits of vulnerabilities, and focus our attention on campaigns. In its simplest form, and widest reach, Kovrr defines a cyber campaign as follows:

> A campaign is an attack targeting computer information systems, infrastructures, computer networks, or personal computer devices implemented by exploiting one or more vulnerabilities. It is designed and executed by a person / group / company with a goal. Common goals are computational assets, theft, intimidation and ideology. The lifespan of a campaign is as long as the time it takes to fix the vulnerability and for most vulnerable devices to deploy a patch, as its effectiveness diminishes as the proportion of previously vulnerable devices, now patched, increases.

* Here we use the terms 'vulnerability' and 'exposure' in the sense understood by the cyber security community, which differs from insurance practitioner terminology. Please refer to https://www.cvedetails.com and to https://nvd.nist.gov/vuln-metrics/cvss for more information.

This definition enables Kovrr to look beyond any specific or hypothetical actions by a threat actor, and also look beyond whether the latter was an APT (Advanced Persistent Threat) or a disgruntled employee. The Kovrr framework defines a set of realistic synthetic events that are capable of generating capital-depleting losses. We can summarize this approach as follows:

- Start with an exploit of one or more vulnerabilities, with the ability to spread automatically or cause systemic issues due to a single point of failure
- Identify all possible goals of threat actors
- The simulation process will design campaigns focused on the goals the exploit is trying to achieve.

Beginning the framework process with exploits and single points of failure ensures synthetic events are realistic. By focusing only on automatically propagating exploits, the synthetic events have the potential to affect large portions of a single portfolio. Additionally, focusing on perpetrator's incentives, allows for generating unseen events that manifest themselves in more complex ways than just ransomware, DDoS etc. The result is a robust event catalog which exposure managers can trust to portray tail cyber risk.

Managing Cyber Risk

Insurance executives are looking for a solution that applies to both silent and affirmative cyber risk. Consistent tools for analysis of both types of risk allow for a seamless transition from silent exposures to affirmative coverages. Additionally, risk should be quantified considering capital modeling and reporting requirements. A consistent approach enables better decision making around deployment, management and protection of capital. Ultimately, carriers aim at eliminating silent cyber and developing strategies around cyber risk in general.

Setting aside bespoke scenarios and PML estimates, the ideal tool for quantifying cyber risk at portfolio level is a catastrophe model. The framework of a catastrophe model is best suited to account for clash across multiple lines of business and multiple coverages. It is also a very familiar framework for practitioners across the industry, who have a duty to validate and confirm a model to be fit for purpose.

Once the framework has been established, other aspects of the model need to be analyzed and put into context. In any case, effective financial quantification of cyber risk across silent and affirmative exposures will require a tool capable of:

- Assessing clash across multiple lines of business and multiple coverages
- Accounting for specific loss triggers
- Dealing with multiple exclusion clauses within the same portfolio

Kovrr's event catalog is built around understanding exploits and campaigns and how they develop into several different types of attacks. The catalog captures correlating traits of a cyber event across multiple lines of business. By building each event from the bottom up, each element of the loss is modeled individually, allowing for a direct link with insurance coverages. Thus, Kovrr's event catalog captures not only the clash across multiple coverages but also specific loss triggers, such as the presence of physical damage for business interruption.

The final ingredient for successful cyber risk management is a solid understanding of how each coverage is affected by the presence of a specific exclusion. In the presence of CL380 for example, Kovrr's approach is to trigger the coverages not excluded, for example, business interruption arising from a non-malicious service provider outage. There are however circumstances where CL380 is likely to be ineffective, such as the case of an attack that didn't intend to cause harm directly to the insured.

This theoretical possibility would need to be settled by a court case following a large event. Experts are already preparing for this possibility and Kovrr's approach allows for some leakage of losses, such as when a service provider outage is caused by a malicious attack.

An easily understood framework and the ability to capture several different aspects of cyber risk are important stepping stones towards the final goal, which is managing capital at risk. To this end the three key advantages of using a catastrophe model are:

- Output is easily consumed by DFA tools and can be incorporated in capital models
- Main drivers of loss can be identified, using different statistical metrics
- Stress tests can be performed at a granular level by altering analysis assumptions and by applying bespoke scenarios.

Stress tests are a useful tool to model hypothetical situations. Kovrr's model explicitly considers the presence of exclusions such as CL380 and others. Users can decide how effective each exclusion is from a standard behavior to a certain percentage of failure all the way to total failure, where the exclusion no longer exists in practice.

Kovrr's Portfolio Management solution allows exposure managers to quantify cyber risk across silent and affirmative. Output is consistent with other catastrophe models, allowing for easy integration with capital models, and the ability to perform stress tests, empowers decision makers to gain valuable insights about the portfolio's resilience to cyber risk.

Conclusion

Cyber is a multifaceted peril capable of generating losses across multiple lines of business and coverages. Silent and affirmative cyber need to be operationalized and managed together. Insurance executives are demanding tools capable of enabling decision making across the board, taking into account capital constraints and the need to deploy capital efficiently.

Kovrr has developed a catastrophe model around a framework that includes concepts such as the potential exploitation of vulnerabilities in cyber attacks and campaigns, where the event set is generated from the bottom up without barriers between different types of events. Tail risk is captured across lines of business, coverages and potential failure mechanisms, and insurance terms include all the most common exclusion clauses, which can be stress tested individually or together.

With Kovrr, exposure managers can now identify and manage cyber accumulations across many sources. Kovrr's modeling techniques allow executives to quantify the impact on capital and make strategic decisions. Additionally, underwriters can now deploy capacity more effectively. Silent cyber is no longer silent, and cyber is on its way to becoming a product, either isolated in one line of business or embedded in several others.

The Author

Marco Lo Giudice, PhD is Head of Pricing Models Development at Kovrr. He has worked in the catastrophe modeling and exposure management fields for thirteen years. Most recently, he served as the Local Head of Pricing at Tokio Millennium Re in the company's UK branch.

CyDelta's Visesh Gosrani & Kovrr's Shalom Bublil, Naomi Weisz, and Tom Boltman also contributed to this report.

KOVRR
Cyber Risk Modeling

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers transparent, real-time data- driven insights into their affirmative and non-affirmative cyber risk exposures. The Kovrr platform is designed to help underwriters, exposure managers and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models.

To learn more please contact the Kovrr team: contact@kovrr.com