

Hidden Risks in Cyber Insurance and How to Address Them

OCTOBER 2020

Introduction

In the last few years, despite an increase in the frequency of cyberattacks, the market has seen cyber insurance rates decline and coverage broaden. This broadening of cyber coverage has led insurers to be exposed to more complicated cyber risks and has increased the complexity in identifying, assessing, and managing aggregations of cyber risk. In 2018, for example, many insurers broadened coverage to include Non-IT vendors of insureds, leaving insurers exposed to a broader range of events. One example is that it increased the covered risk to include a workforce management platform for the supplier of the insured. If the supplier was then targeted by a cyber event that caused disruption to them and consequently the insured; this event would now trigger a business interruption claim.

Other examples of the increasing reach of aggregation can include payroll and accounting software that might lead to privacy claims, as well as aggregations of underlying content delivery networks and other critical network points of failure.

In addition, a number of factors are constraining the market's capacity to write business. These include regulatory concerns around capital adequacy related to the Covid-19 pandemic, as well as Lloyd's efforts to reduce poor performance across all business lines.

As insurers finalize a renewal strategy within this context, it is important to more accurately understand the expected performance of individual policies. This will enable them to calculate a long term loss ratio. When taking the long term loss ratio into consideration alongside other renewal factors (such as customer relationships, catastrophe concentrations, company, and industry concentrations), insurers can make more data-driven decisions for their renewal strategy focused on policy profitability.

Policy Renewal

When considering renewing policies, most insurers can place their business into the following five buckets which then drives their renewal approach. Note that discounting is not recommended below, however, it may be appropriate in some circumstances.

Bucket	Renewal approach
Significantly better than target loss ratio	Write the policy again at a flat rate
Better than target loss ratio	Write the policy with a small uplift but be prepared to stay flat
In line with target loss ratio	Write the policy with a small uplift
Poorer than target loss ratio	Apply at least the minimum market norm uplift and try to bring closer to target loss ratio
Significantly poorer than target loss ratio	Apply a significant uplift or decline to renew

In addition to the usual factors used to make decisions around renewal options in each bucket, access to the following data can bring to light unique aggregations within a portfolio and alter renewal decisions:

- + Loss ratio per policy
- + Diversification effect of new policies
- + Risk characteristics which further add to high aggregation points within the portfolio
- + Catastrophe element of the expected long term loss ratio



Loss Ratio Per Policy

To fully understand the extent to which each policy contributes to normal portfolio performance and adverse risk, insurers need to calculate the expected loss ratio per policy and the extent to which this might vary. Enhanced visibility of the cybersecurity posture of the companies insured can allow for greater precision in understanding the risk and thus the portfolio's exposure to attritional, large loss, and catastrophic cyber events.

In order to calculate the loss ratio per policy, one needs to calculate a long term loss ratio using simulation techniques and to take into consideration the premium collected. Segmenting by profitability in this way, allows insurers to steer their portfolios and provide better underwriting guidelines.

Diversification Effect of New Policies

In order to better diversify an existing book, an insurer would need to know which scenarios are likely to affect multiple companies. One way to do this is to quantify whether a new policy correlates with existing risks or if it adds diversification to the existing policies in a book. This is important to reinsurers thinking about how a book of business diversifies against their other books, and to primary insurers writing higher limits.

Kovrr identifies the main contributors to the annual average loss and to the events driving the tail. This allows exposure managers to understand how potential hidden aggregation stacks up to substantial damage caused by multiple small events ("death by a thousand cuts"), or which events cause significant damage to a large part of the portfolio at a single point of time.

The Kovrr platform can surface the areas of greatest risk aggregation. For example, there are many common technologies that are shared by a majority of clients, such as a Windows operating system for employee endpoints. However, obscure third-party libraries or service providers that power other products can often lead to an unintentional aggregation significantly out of line with their market share. Awareness of this enables insurers to consider if they wish to reduce these exposures.

Risk Characteristics Shared with High Concentration Aspects of the Portfolio

In cyber risk, understanding the underlying technologies and services used by companies within the portfolio is key to understanding avoidable aggregations. These aggregations concentrate your exposure to a single risk which may lead to greater losses than expected if that risk were to be triggered. Use of cloud services is one such example. Small- to medium-sized businesses in the legal and accounting industries in the United States are likely to use Azure cloud services, but other specific industries

have a tendency to use Amazon Web Services. While portfolio managers may be expecting a particular aggregation in a cloud provider such as AWS, there may also be more obscure aggregations, which can be useful knowledge for managing their portfolio's exposure.

Kovrr has identified three cyber risk elements: location, industry, and entity size. The CRA-Zones™ framework defines the minimal elements needed to provide a view of aggregated cyber exposure. CRA-Zones allow for analysis across multiple portfolios of risks and monitoring of exposure trends.

Insured risks with these characteristics in common will tend to “occupy” the same, or neighboring, CRA-Zones. They tend to be exposed to similar types of cyber issues, and therefore potentially contribute to cyber catastrophe events. They are likely to have cyber proximity, similar to geographical proximity within a CRESTA Zone.

Additionally, applying the limit per CRA-Zone enables insurers to show particular concentrations or, conversely, that their risk profile is spread across a large number of risks.

Catastrophe Loss Ratio

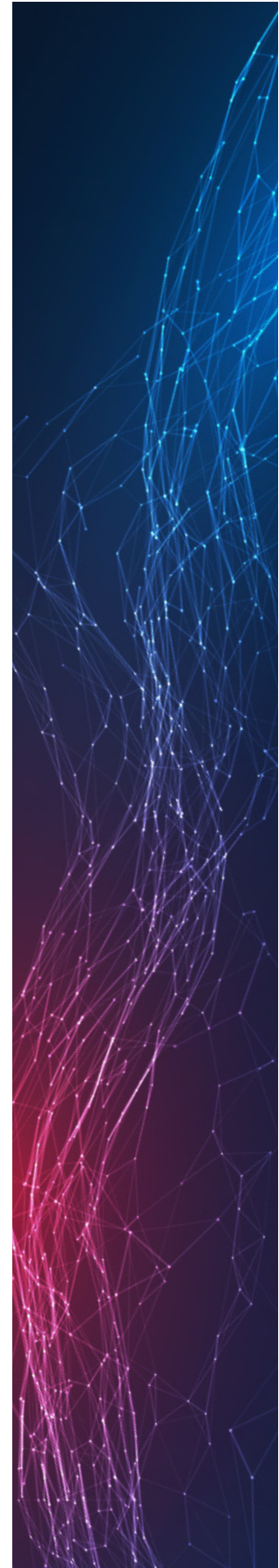
Understanding the proportion of the loss ratio that relates to catastrophic events enables better alignment of the renewal portfolio with your risk appetite.

This proportion can vary significantly by industry. A healthcare institution could have significant losses due to a negligent breach of health data, whilst a data breach at a charity is likely to be less catastrophic in terms of the data's value.

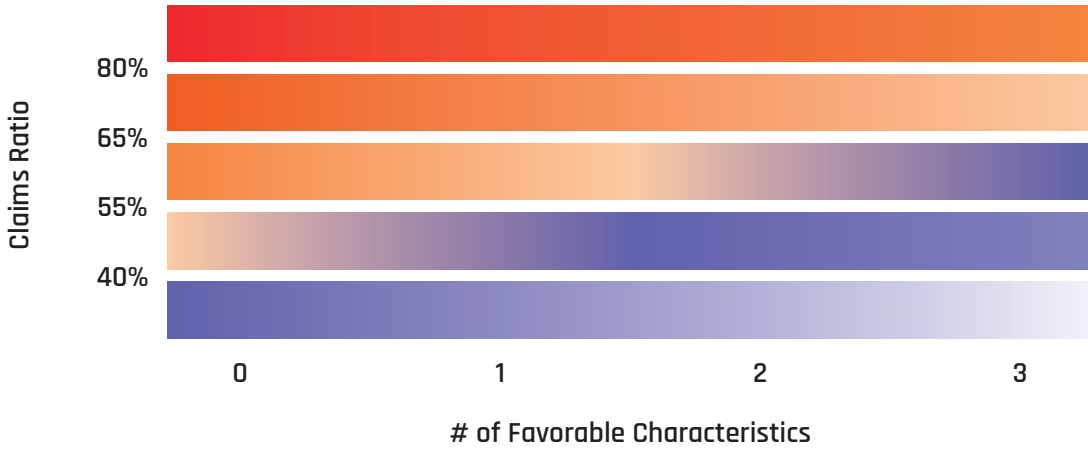
However, even within the healthcare sector, a particular institution could be more vulnerable to catastrophic cyber events as a result of its hardware and software infrastructure and configuration. This may make it more susceptible to the data breach or make it a more attractive target. Both the catastrophe exposure of different industries and between industry peers are relevant when considering which risks are more attractive at renewal.






Gathering the information above will help segment policies according to profitability levels. In order to illustrate an example decision process below, numbers have been applied to represent reasonable “claims ratios.” The use of these numbers is in no way suggesting what claims ratios should be for an organization. Kovrr recommends tailoring these numbers to your organization's preferences. This will enable proper segmentation according to your organization's risk appetite and other elements related to your company's cyber risk exposure.

Given the general increasing level of cyber threat, Kovrr would recommend against actively discounting unless the expected loss ratios are significantly favorable. This is because this ensures it is easier to retain flat rates or limit price increases going forward.



Below is an example based on a hypothetical target claims ratio of 60%, segmenting existing policies into five buckets:



- A  Significantly better than target loss ratio
- B  Better than target loss ratio
- C  In line with target loss ratio
- D  Poorer than target loss ratio
- E  Significantly poorer than target loss ratio



A. These policies are significantly better than target loss ratio. Write again at flat rates or write at some discount.

When rates are significantly below the target claims ratio, if the other elements taken into consideration are also positive and policy coverage is not being broadened, it is key to ensure that the policy remains within the insurer’s book. Therefore, it may be sensible to discount upfront or in a negotiation to ensure the policy is retained.



B. Write with a small uplift or stay flat.

When rates are below the target claims ratio and other characteristics are positive, some discount could be considered in negotiation in order to retain the policy. However, by staying flat or even, if possible applying a small uplift, this enables any future price rises to remain limited.



C. Write with a small uplift.

As per bucket B, it is sensible to uplift the price, but if the loss ratio is favorable and other characteristics are positive, staying flat might be considered in negotiation in order to retain the policy.



D. Write with an uplift to bring the insurer closer to their target claims ratio.

If other characteristics are adverse and the renewal strategy is working well, it may be worth declining to renew. If other characteristics are positive then the level of uplift might be considered to such a level that would bring the insurer closer to their target claims ratio over a two to three year period.



E. Decline to renew.

If other characteristics are favorable, renew with a sufficient uplift to bring the insurer closer to breaking even, with the intention to continue the increases.

Conclusion

At the same time that the market is experiencing increasing cyber insurance rates, some insurers are constrained in the extent to which they can take advantage of the premium rate rises. This creates an opportunity for portfolio optimization for insurers who have, until now, been following a year on year growth strategy. When considering renewing policies, insurers can combine their traditional considerations with additional data points to better target rate rises and potentially apply reductions to retain the best risks.

The Kovrr platform can be used to calculate expected loss ratios by policy, gain quantitative and qualitative insights on aggregations of technologies and services used, understand the catastrophe element of loss ratios, and gain additional insight on the policies that can better diversify their portfolio.

The Authors



Shalom Bublil

Shalom is Chief Product Officer at Kovrr and a cyber data science expert. Throughout his career, Shalom has acquired unique expertise in cyber intelligence, threat modeling, risk modeling, machine learning and artificial intelligence. Shalom joined an elite Israeli intelligence unit and served for four years specializing in cyber. Following his military service, he joined Lagoon Mobile Security where he led the threat intelligence and threat modeling initiatives. In his last position before founding Kovrr, he led cyber threat intelligence and modeling efforts at Deep Instinct, developing a commercial detection engine product from scratch based on advanced artificial intelligence technology. Shalom holds a B.A. from the Open University of Israel.



Visesh Gosrani

Visesh Gosrani is Chair of the Institute and Faculty of the Actuaries Cyber Risk Working Party. He has over 20 years of experience as an actuary and Chief Risk Officer in the insurance industry. He also co-founded Shoal, which was acquired by Cyence. After the acquisition, Visesh was named Director of Actuarial and Risk at Cyence and continued in this role after Cyence was acquired by Guidewire. Prior to working for Cyence and Guidewire, Visesh was Chief Risk Officer for Asta, a Lloyd's of London Managing Agent, Actuarial Leader for Genworth and a Consulting Actuary for Deloitte and PwC.

Kovrr's Naomi Weisz also contributed to this report.

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers transparent, 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