Are insurers adequately balancing risk & opportunity? Findings from PwC’s global cyber insurance survey
Introduction

In light of recent, major cyber-events, companies in all industries are increasingly aware of the potential threats to their businesses, as well as associated risk mitigation and cyber security techniques. Headline generating attacks show that cyber threats are becoming more sophisticated and aggressive. In this context, the market for cyber insurance continues to grow. The current US standalone cyber insurance market is estimated at $2.5 - $3.5 billion annually and is expected to grow by another $2 billion over the next three years.¹

The cyber market recently has seen an influx of new entrants. This is likely the result of market-wide favorable combined ultimate loss ratios, which has created additional capacity and in turn a softening market. In this soft market environment, we have observed increasing overall limits. Furthermore, sub-limits such as (contingent) business interruption ((C)BI) sub-limits, are increasing or no longer included in contracts.

It is still unclear whether or not cyber risks are adequately priced given the increasingly systemic and extreme nature of cyber-attacks. The inevitable market-turning event will separate carriers that have sufficient risk management, underwriting processes and capital in place from ones that do not.

We recently completed a global survey of specialist writers active in the cyber market. We describe in the pages that follow key conclusions from the survey results.

The majority of respondents indicated to have claims data from incidents like data breach, ransomware, malware and phishing. The average number of years of available data is approximately seven years.

Insurers should exercise caution when relying on cyber data, as its quality and granularity is highly variable, and it is almost certain that cyber threats of the future will be different from those of the past. This means that data may become outdated or irrelevant as carriers start using it in underwriting and modelling.

For example, tech errors and omissions (E&O) data is sometimes used in lieu of actual cyber claims data, but they are actually different in nature. BI and CBI covers are the main protections that insureds seek, yet cyber-related CBI claims data is extremely sparse.

In the past, first party claims would blow through entire insurance programs. Increasing limits in combination with reducing sub-limits may now mean that cyber writer’s exposures are shifting further towards slower developing third-party claims than is present in historical data.
Because of its potentially systemic impact, cyber related business interruption/contingent business interruption is the scenario that most worries companies.

Figure 2 Challenges in cyber accumulation

Survey respondents identified parameterization of potential maximum loss (PML) as one of the greatest challenges in cyber accumulation management. As the industry pushes for improved cyber modelling practices, it will better understand and more accurately quantify the potential for BI/CBI accumulations.

We also note that survey respondents identified data breach or cyber ransomware scenarios as less concerning because of the 1) increasing availability of related, enhanced threat data, and 2) limited scope of the systemic impact of such a scenario.

Cyber BI/CBI is a relatively untested risk coverage for (re)insurers and, due to its complex nature, particularly challenging to underwrite. Nevertheless, we anticipate strong growth of BI/CBI cyber covers, driven by increased demand from insureds following recent cyber incidents like NotPetya. This growth will further increase with, for instance, customization of covers through broader policy wording.

—

2 NotPetya was a 2017 cyber-attack that, on the surface, appeared as a (Petya) ransomware attack. However, instead of the typical ransomware mode of action, NotPetya was designed to spread fast and cause damage; it was built to destroy rather than to extort.
The majority of respondents to our survey reported that they are writing business at combined ratios lower than 80% for the most recent annual period, highlighting the current profitability of these books.

The majority of respondents’ actual combined ratio is stronger than or in line with their initial target, suggesting that the majority of the respondents have achieved their target premium level. Despite a small number of firms being below their growth target, the appetite to grow the cyber book is very strong.

While the combined ratios insurers report in our survey currently suggest healthy product profitability, new market entrants and competition are likely to erode it. The insurance industry has yet to experience a major and systemic cyber catastrophe event. Accordingly, we note that reserves and claims may develop adversely in time, and future profitability may be lower than insurers currently expect.

In addition, carriers are increasingly worried about any potential claims from non-affirmative policies (“silent cyber”) and how they may affect their current reserve levels.
Companies are actively using reinsurance to manage the growth of their cyber exposures, with over 75% of companies transferring risk to reinsurers. No respondents indicated using non-proportional reinsurance at the time of the survey.

The majority of respondents to our survey are seeking to transfer risk above a pre-defined retention level. The design of non-proportional reinsurance structures requires a robust quantification methodology, an understanding of the exposure accumulations, confidence in pricing, and a clear definition of what constitutes a cyber event.

Accordingly, there is a greater appetite for proportional reinsurance, where reinsurers can rely on a cedants’ underwriting expertise to create an alignment of interest, rather than model results they do not trust.

In some instances, cyber exposures will be covered on a non-proportional basis through property insurance (PI), directors and officers (D&O) and E&O programs, where cyber acts as an ancillary exposure. As quantification capabilities mature, we expect to see more diversified capacity coming into the market, including insurance linked securities (ILS).
Conclusion

Although the cyber market presents a significant opportunity for insurers to profit in a soft market, they need to be aware of the significant risks and downside potential to writing this business, including limitations in historical data and uncertainties in accumulation risk. It is very important to underwrite risks at the right price. This means that proper underwriting guidelines have to be in place, and pricing models need to be as robust and reliable as possible.

Due to the continuously changing nature of cyber threats, a scenario-based modelling approach is crucial. Model validation and robust model risk management processes also are vital for a model to remain appropriate and sustainable in the face of constantly changing threats. Moreover, we expect regulators to require more robust validation of cyber modeling in the future. To cope with these increased requirements, internal validation teams may need training on this new and specialized area.

Insurers should also consider becoming more hands-on and work directly with insureds in their risk mitigation and reduction efforts – for example, by helping them tighten internal controls and improving cyber related training and awareness.