RESEARCH BRIEF

Advancing Accumulation Risk Management in Cyber Insurance

THE GENEVA ASSOCIATION

Prerequisites for the Development of a Sustainable Cyber Risk Insurance Market

Daniel M. Hofmann, Senior Advisor Insurance Economics, The Geneva Association
Steve Wilson, Senior Advisor Cyber, The Geneva Association

In collaboration with Rachel Anne Carter, Director Cyber, The Geneva Association

Although cyber risk premiums have expanded sizeably in recent years and loss ratios compare favourably relative to other product lines, sustainable growth of the cyber insurance market should not be taken for granted. A report issued by The Geneva Association identifies three prerequisites that must be met to ensure sustainability.[1] Despite recent advances, cyber risk creates unprecedented challenges. But the report is nevertheless cautiously optimistic that cyber insurance can become manageable over time.

Prerequisites to ensure the sustainability of cyber insurance

Expanding the boundaries of insurability and making new risks manageable is not new for the insurance industry. Over centuries, insurers have developed products and services that reflect the changes in the risk landscape.

Cyber risk is nevertheless taking us into uncharted territory. Exposure bases are hard to define and measure, and they are constantly changing. Historical claims data are scarce and not considered to be well representative of future vulnerabilities. Threats are constantly evolving; they can spread widely and rapidly, and a series of consecutive large events is plausible. Moreover, a high degree of interconnectivity may result in potentially boundless impacts. Thus, to make cyber risk insurable, three fundamental prerequisites must be met.

- ***First***, there needs to be sufficient resilience at the source of risk. If homeowners did not lock their homes, theft would not be insurable. The first steps in addressing any risk are to assess, measure and manage it. Residual risks (i.e. those that cannot be contained at the source) can then be mitigated through insurance.
- ***Second***, insurers must make an acceptable return on capital. This requires disciplined and effective underwriting.
- ***Third***, the available capital must both withstand shocks from accumulation events and provide adequate compensation to insureds after such an event—in the case of cyber, it means absorbing accumulation risk, which is the root of many concerns about cyber risk.

This research brief reviews the industry's progress in addressing the third prerequisite, i.e. the many challenges created by accumulation risk.

Improvements in underwriting capabilities

At the core of all underwriting is the need to know the exposure, which is a measure of risk. In property classes, exposures are readily measurable and stable over time, but in the digital economy, exposures are neither stable nor measurable.

With the difficulties of measuring exposure comes the double challenge of assessing claims cost. First, historical claims data are sparse. Second, threats are changing rapidly. They spread and replicate across the globe and, unlike natural catastrophes, can endlessly adapt and recur with alarming frequency. So even with a credible volume of historical claims data, its predictive power is questionable.

To address these challenges, insurers have developed a number of approaches.

- To improve exposure measures, data protocols are emerging that combine basic company information with digital risk indicators, such as patching frequency and backup procedures. In 2016, Lloyd's established a schema for cyber exposure data that provided a much-needed standard for the key features of input data in cyber risk tools and the attributes to be considered when evaluating cyber risk.[2]
- Advanced data analytics allow the analysis of special cyber risk characteristics. Service providers have developed digital risk assessment tools, providing risk scores and benchmarks of standards compared to peers. While there is a potential for promising insights, the tools will undoubtedly take more time to mature.

1 For the full report see https://www.genevaassociation.org.
2 See https://www.lloyds.com/market-resources/data-and-research/cyber-core-data-requirements.

- Leading underwriting organisations are also implementing proactive approaches to assess the likely rate of change in future developments. It is now accepted practice for insurers to draw on a range of inputs, such as research publications, specialist modelling firms, and cyber security companies. Accumulation modellers may also conduct their own research and discuss trends with in-house cyber security experts. In larger insurance companies, the risk engineering function is evolving to include cyber and technology skills.

The common thread to these developments is the shift from an essentially 'physical' world to a 'digital' world. The future underwriting profile will likely include a deeper understanding of data sciences and a much greater familiarity with the technologies at the source of the underlying risk.

Towards more sophisticated modelling

Currently, insurers rely on pragmatic—but solid—methodologies that assess proportions of total limits at risk against the currently known major scenarios of data breaches, cloud outage, widespread malware, and disruption to critical infrastructure. These deterministic, scenario-driven methods, with expert judgement applied, provide a working solution while more sophisticated and insightful models are being developed. Progress is being made, but there is a divergence of views.

- ***For the bears***, the challenges are highly significant and will take a decade or more to overcome. Should this view prevail, capital providers may be unwilling to provide funds at the levels needed to support expected market growth.
- ***The bulls***, however, believe that advances in technologies will provide the capabilities to understand and measure these new technological risks. In this view, data, far from being scarce, is abundant and it is only a matter of how to extract, capture and utilise it. Techniques are emerging that harness the computational power of today's data processing and analytical tools and so shorten the duration of the learning curve for cyber risk, with maturity perhaps around five years away.

Both views have their proponents, and both have compelling arguments. Progress will likely depend on insurers resolving three major challenges.

The first challenge is to even define a '*footprint,*' let alone measure the exposure within it. Supply chains have become increasingly digitalized and, with the range of cloud-based services extending further along the value chain, aggregations 'in the cloud' lie both within and across industries. And the Internet of Things creates connections that reach into the homes of hundreds of millions of individuals. These connecting threads and digital 'monocultures' create an exposure base that is largely opaque, lacks hard boundaries and enables threats to permeate across sectors and countries.

The second challenge relates to the *scarcity of extreme events*. Modellers of natural catastrophes have addressed the 'data scarcity' for many natural perils by reference to relevant sciences, such as meteorology and seismology. However, for cyber modelling, there is no analogous hazard science to draw on.

The third challenge is created by the high level of *interconnectivity*. Cloud service providers now connect many commercial organisations that would otherwise have little or no dependency. Further, commercial entities use common software or basic hardware. These monocultures create connecting threads both across and within industry sectors and present unprecedented challenges for risk assessment.

However, in the light of these challenges, seemingly intractable problems have become more tractable in recent years.

- One approach uses publicly accessible digital information to identify connections between firms and their cloud providers. With a detailed digital map, it is then possible to assess the impact on a business of a specific cloud outage or failure, a significant step in understanding the risks associated with cloud interconnections.
- An annual study by Verizon, based on a set of nine common attack patterns and an extensive event database, shows that attacks have tended to cluster by industry sector.[3] This is promising and suggests that the 'footprint' problem is not intractable.
- Novel approaches are emerging to address the challenges of malware attacks. One modelling firm is looking at the link between pandemic and cyber risks and is exploring similarities between the mathematics of epidemiology and the spread of viruses, worms and malware through computer systems. Understanding these patterns enables the modelling of such risks and a 'footprint' which can be adapted to the cyber space.
- Various reports covering accumulation scenarios and the work being done internally by insurers indicate progress in understanding the potential severity of major events. But being able to estimate the severity of events is not sufficient, and managing accumulations to worst-case scenarios will lead to a conservative position on risk acceptance, potentially limiting capital allocated to this market.
- Regarding claims, although empirical data are often claimed to be scarce, there are substantial volumes of information on data breaches, and the growing number of significant actual events or 'near misses'—such as the ransomware attack WannaCry, the Dyn distributed denial of service attack, and system flaws such as Meltdown—provide valuable data points that allow for a novel understanding of cyber risk.

3 Verizon (2018).

- Counterfactual analysis, the discipline of reimagining historical events how they might have been or how they may differ should a similar event occur in the future, is another technique adding to the understanding of potential accumulations.[4] A transparent and well-structured analysis may provide a richer texture to data-poor models, and so-called 'downward counterfactuals' (where worse outcomes are imagined) can contribute towards a better understanding of likely extreme loss scenarios.

These developments indicate tangible progress. Cyber catastrophe models are progressing beyond the pragmatic 'stacking of limits' and they are starting to have many of the qualities of their natural catastrophe counterparts. That said, much more needs to be done for accumulation models to reach standards comparable with natural catastrophe modelling.

A risk assessment

The history of cyber risk is short, and the market has yet to experience a major adverse event. It is vulnerable to risks, and without due attention there is a potential of slipping into undisciplined underwriting.

- A single major event, or a series of consecutive events, could generate losses large enough to render the market unprofitable, inducing (re)insurers to withdraw. It could alternatively induce them to introduce tighter policy terms and in doing so increase the number of exclusions and/or make buy-backs prohibitively expensive. Likewise, underestimation of exposure, especially nonaffirmative, could result in significant, unanticipated losses.
- The lack of confidence in advanced models could stifle growth if they are deemed to be too blunt for insurers to extend portfolios or offer higher coverage levels. A negative swing in perceptions towards a less profitable and riskier market could also leave the market for small and medium enterprises underdeveloped. A large event may also trigger regulatory intervention with the risk of insurers having to provide cover with uneconomic terms and rates.
- Lack of discipline in policy wording, especially to control exposure to acts of terror, is a key concern. Under such scenarios, a sizeable withdrawal of market capacity could ensue, with tighter policy conditions, wider exclusions, and price hikes in cyber-specific covers.
- Of equal importance is the need to maintain underwriting discipline. Cyber risk is not unique in this respect. Historically, many property and casualty classes have suffered when underwriting standards slipped or when prices failed to adequately reflect the cost of risk. Many insurers perceive the current rating environment as soft and likely inadequate should any of the above risks materialise.

Table 1 Challenges and responses in the cyber insurance market

Cyber characteristic	Capabilities impacted	Industry response	Ongoing issues
Exposures hard to define and measure; constantly changing.	Exposure measurement.	Establishment of core data schema; Digital risk assessments at the insured level.	Technical nature of exposures very different from other classes—difficult to learn and creates talent issues.
Claims data scarce and not representative of future vulnerabilities.	Claims assessment; Modelling.	Utilise breach data and publicly available data on major events to generate scenarios.	Insurers may be wrong-footed by unseen threats or trends deviating from expectations.
Threats evolve constantly, spread widely and rapidly, and can recur.	Claims assessment; Modelling.	Forward-looking threat assessments including external expert inputs; Develop in-house technical know-how	
Highly interconnected with potentially unbounded exposure.	Accumulation modelling.	Mapping cloud and digital supply chains; Machine learning (ML) for complex relationships between exposure and claims.	Malware still a major threat; Non-affirmative cover exposure not assessed; Yet to assess ML effectiveness.

4 Lloyd's and RMS (2017).

All stakeholders must step up

The insurance industry can offer only a partial remedy. Other stakeholders must play their part too. Given the fluid stage of developments, it would nevertheless be premature to make firm recommendations. Prudence suggests to refrain from making irreversible decisions, especially when a market is demonstrating high levels of innovation. Policymakers should endeavour to use the market as a discovery mechanism and expect best practices to be adopted quickly by competitors and new market entrants.

There have been a number of policy recommendations under discussion. They include extending the coverage provided by terrorism pools in the countries where cyberterrorism coverage has not yet been offered. Additional governmental backstops related to cyber losses (beyond losses triggered by terrorism) could signal to the market that the public sector too has 'skin in the game' and is prepared to contribute to solutions developed in the private market. To strengthen resilience, cyber security features should be developed and implemented at inception, and security design features should be certified and controlled by authorities. Jointly with IT security providers and insurers, authorities should develop and implement foundational IT and information security standards that facilitate IT security hygiene. Governments could also consider becoming signatories to a 'Digital Geneva Convention,' which would contain the use of cyber weapons by governments.[5]

References

Lloyd's and RMS (2017) What if…? How reimagining history could help insurers better analyse risk, available at https://www.lloyds.com/news-and-risk-insight/press-releases/2017/10/what-if

Microsoft Policy Paper, A digital Geneva convention to contain cyberspace, available at https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace

Verizon (2018) Data Breach Investigations Report: Tales of dirty deeds and unscrupulous activities, available at https://www.verizonenterprise.com/verizon-insights-lab/dbir/

5 Such a non-proliferation convention was recently proposed by Microsoft (2017).