CyberCube

ILS AND THE CYBER MARKET: UNLOCKING POTENTIAL IN THE CAPITAL MARKETS

JANUARY 2020

Authors:
Laurel Di Silvestro, Principal Client Services
Matthew Silley, Client Services Manager
Rebecca Bole, Head of Industry Engagement

Editorial Manager:
Yvette Essen, Head of Content & Communications

Catastrophe Modeling: The Key to Unlocking Growth in Cyber ILS

For the past 20 years, the capital markets have offered crucial capacity for certain catastrophe-prone perils and regions where traditional insurance and reinsurance capacity has been hard to secure at acceptable terms and conditions.

There is a growing consensus that there are certain peak cyber perils defined as accumulations of exposure in a common technology or software that could have systemic impact if compromised. For these peak risks, there is expected to be a need for the capital markets to provide alternative insurance-linked instruments to alleviate the catastrophic financial impact of cyber-related events.

However, the cyber (re)insurance market is still relatively immature and capital market investors are just beginning their education on the potential financial impacts of systemic cyber events to the (re)insurance industry.

“Insurance-Linked Securities (ILS) investors sense an opportunity in the cyber risk market but are still treading carefully in this fast-evolving landscape.”

Insurance-Linked Securities (ILS) investors sense an opportunity in the cyber risk market but are still treading carefully in this fast-evolving landscape.The cyber insurance market offers a compelling route to portfolio diversification and strong returns, with limited correlation to other asset classes.

ILS has already branched into areas such as life, accident and health. Additional popular ILS instruments include property & casualty (P&C) and specialty classes, including aviation, energy and marine that offer new interconnected multi-class opportunities. Importantly, increasing confidence in the value of cyber ILS solutions is evidenced by a couple of active cyber ILS transactions in the market, and the formation of working groups to develop cyber indices.

Investors understand that portfolio level probabilistic cyber risk models are key to delivering the modelled loss and other cyber risk metrics required for ILS transactions - regardless of the trigger type (see appendix). But they require a deeper understanding of the risk before they can start to dive into modelling techniques and data, assumptions and methodology, which will be key to narrowing the cyber protection gap.

In support of this increasing interest, CyberCube is engaging with the reinsurance industry to determine how an ILS cyber modelling solution might be constructed - given there are unique features of cyber risk that pose challenges to the development of an ILS product.

Same, Same, but Different

Cyber catastrophe risk is distinct from the natural catastrophe risk market in terms of the maturity of the insurance market experience and how the risk is quantified today:

- There is a lack of well-defined historical cyber claims data, making quantification of cyber risk more difficult
- Insurance cover is not standardised or fully explicit in all insurance policies. The impact of this non-affirmative cyber cover is difficult to quantify
- The cyber insurance market has not yet suffered a systemic, catastrophic-level event that has threatened the profitability or solvency of carriers. However, it is widely accepted that as the digital economy becomes more interconnected, the probability of such a large event occurring is increasing
- With no precedent for a market consensus cyber catastrophe loss, there is an increased need for credible and robust cyber catastrophe modeling. Cyber risk carriers need to understand the potential scenarios that might cause a loss and the frequency and severity of the financial impact of those scenarios on (re)insurance portfolios
- The constantly changing cyber risk and threat landscape further clouds the digital cyber picture, as risk parameters change over the duration of an insurance-linked instrument
- Another concern is how best to characterize the cyber ILS trigger type and amount for a bond pay out. Indemnity triggers, for example, have a long claims pay-out tail that is further complicated by non-affirmative or “silent” cyber risk that can cross over into multiple lines of business. A good example of this type of risk is the NotPetya attack in 2017, which resulted in claims under property and Director and Officer’s (D&O) policies, among others.

Building an Industry Loss Index

One development that could build confidence in cyber ILS is the existence of an industry loss index - a referenceable portfolio of data points that can indicate trends or be used as the basis for a loss trigger in insurance-linked instruments.

A CyberCube/Guy Carpenter white paper titled "Looking Beyond the Clouds" published in September 2019 created a synthetic portfolio of US affirmative cyber insurance exposures and estimates industry losses from various catastrophe scenarios.

The portfolio represents $2.6 billion in affirmative cyber insurance premiums and has been used to estimate US insurance industry losses from cyber catastrophes developed in the CyberCube Portfolio Manager risk aggregation model.

Property Claim Services (PCS) has also developed an industry loss index and estimates service for cyber (re)insurance, covering losses that involve multiple insureds across affirmative and silent cyber with industry-wide insured losses of at least $250 million.

It should be noted that there is some wider activity around developing cyber indices. For example, the ASTIN working party is researching what a cyber index might look like, and there are some active cyber ILS transactions which have various triggers in play.

Cyber Scenario Case Study

How a catastrophic cyber aggregation event is defined is another significant component of the structure of ILS products. Solutions are increasingly focused on quality data sources and sophisticated analytics that include identification of technological vulnerability dependencies, scenario-specific single points of failure, and those that are developed with a structured approach that credibly define what could happen in an evolving risk landscape.

"An ILS cyber deal could provide a specific level of cover over and above a pre-defined portfolio loss attachment point relative to a clearly defined scenario."

The view taken by the authors of this paper is that the first cyber ILS deal will look much more like a traditional event cover, with the caveat that intangible, complex risks of this nature are hard to define.

An ILS cyber deal could provide a specific level of cover over and above a pre-defined portfolio loss attachment point relative to a clearly defined scenario. For example, Carrier A is concerned about cloud outage. A third-party capital investor will provide $250 million of cover sitting in excess of a $250 million net of traditional reinsurance portfolio loss in the event of a 12-hour outage from a major cloud provider such as Amazon Web Service, Azure, or Rackspace.

CyberCube Solutions

Cyber risk is a dynamic, man-made peril that is evolving rapidly. The motivations of cyber attackers, their methods and the technical vulnerabilities they exploit are constantly in flux. Developing a robust, forward-looking view of risk in portfolios is a complex and resource-intensive task.

The forward-looking nature of cyber risk creates increased uncertainty for risk modelers and ILS investors trying to determine loss parameters and develop realistic cyber catastrophe scenarios. ILS investors need flexibility to vary frequency, severity and other assumptions to dynamically stress test model outputs.

ILS transactions require dedicated “depth of field” specialist support for analysis of the risk. CyberCube is uniquely qualified to provide that support for cyber risk transactions. This expertise is underpinned by probabilistic loss models based on unique inside-the-firewall data as well as best in class quality analysis of outside-the-firewall data. Inhouse cyber risk knowledge, data analyst insights and access to key cyber risk experts and industry partners provides additional subject matter expertise.

CyberCube has developed portfolio level probabilistic cyber risk models, of the type that will be key to delivering the modelled loss and other cyber risk metrics required for ILS transactions.

Our solutions focus on the development of quality data sources and sophisticated analytics that are at the level of detail required for traditional ILS transactions. The models include identification of technological vulnerability dependencies, scenario-specific single points of failure, and scenarios that are developed with a structured approach that credibly define what could happen in an evolving risk landscape.

In addition to in-house cyber risk and data analysts, CyberCube works closely with key industry partners that deliver access to industry data and cyber experts that inform and provide critical resources for the structure of ILS products.

Conclusion

The potential for growth in cyber insurance is enormous and presents a significant opportunity for capital providers to gain diversified returns on their investments.

Unlocking this potential will require collaboration from across the broking, carrier, investor and risk modeling communities. CyberCube is committed to engaging with ILS stakeholders as we continue our journey of discovery and education on cyber risk modeling and the development of insurance-linked instruments.

Author:

Laurel DI SILVESTRO, Principal Client Services
Matthew SILLEY, Client Services Manager
Rebecca BOLE, Head of Industry Engagement

Editorial Content:

Yvette ESSEN, Head of Content & Communications at CyberCube

APPENDIX

Common Types of Insurance-Linked Instruments

There are four main types of ILS instrument:

The catastrophe bond which uses an indemnity trigger based on portfolio event claims from the cedant's exposures.
"Cat bonds are an example of insurance securitization to create risk-linked securities which transfer a specific set of risks (generally catastrophe and natural disaster risks) from an issuer or sponsor to investors. In this way, investors take on the risks of a specified catastrophe or event occurring in return for attractive rates of investment. Should a qualifying catastrophe or event occur the investors will lose the principal they invested and the issuer (often insurance or reinsurance companies) will receive that money to cover their losses." (Source: Artemis)

Industry Loss Warranties (ILW) are based on industry loss indices.
"An industry loss warranty, known as industry loss warranties or ILW's, is a form of reinsurance or derivative contract through which a company or organisation (often an insurer) can gain coverage based on the total insured loss experienced by the industry rather than their own losses from a specified event. The contracts have a specified limit which denotes the amount of compensation the buyer receives if the industry loss warranty is triggered."(Source: Artemis)

Parametric cover is a binary trigger, based on pre-defined terms.
"Parametric insurance or parametric risk transfer is a type of insurance, reinsurance or risk transfer arrangement that does not indemnify the full loss for the protection buyer… a party is buying a pre-defined amount of protection which will pay-out based on pre-defined terms… A trigger mechanism defines when the contract is to pay-out to the protection buyer. This trigger is typically based on parameters directly related to the risk that the protection buyer seeks to acquire coverage against." (Source: Artemis)

Sidecars and collateralized reinsurance are most closely related to traditional (re)insurance cover. Sidecars are fully-collateralized joint venture vehicles between third-party capital and a (re)insurer. The sidecar vehicle allows (re)insurers to easily access alternative capital to support their underwriting. Collateralized reinsurance allows third-party capital to participate directly in reinsurance contracts. The collateral normally amounts to the full potential claims that could arise from the reinsurance contract.

Other less common triggers exist, such as modelled loss to a portfolio.