Drawing from the Experience of Nat Cat Modeling

Changing Cyber Risk Landscape Creates Need for Multi-Faceted Approach

CyberCube

www.cybcube.com

The cyber insurance market can learn lessons from the experiences of the natural catastrophe insurance industry, although the unique characteristics of cyber risks mean that there are as many differences as there are similarities for this risk compared to natural catastrophe modeling.

Parallels and differences can be drawn across both sectors when modeling these risks. A huge amount of progress has been made since natural catastrophe models were first introduced 30 years ago. The paths of insured loss accumulation are well understood through a significant volume of historical scientific and claims data, such that the limitations of such modeling are acknowledged and documented. While the (re)insurance industry faces challenges when taking into account the evolving impact and understanding of natural catastrophe risks (most notably climate change impacted models), the rapid pace of evolution in the recent man-made world of cyber risk perils does not allow the same opportunity to observe, learn, and adapt from past data and models.

The insurance industry now relies heavily on catastrophe modeling to set capital adequacy, adhere and respond to evolving regulatory requirements and stress testing. Key areas of focus include how models have developed and can be deployed within an insurance company, the way in which regulators are looking at models and how they are utilised to help with capital allocation within insurance companies.

> **"We can learn from the experience of the Nat Cat modeling world, its evolution and interface with the insurance sector"**

Cyber risk insurance has only been a meaningful market for less than 15 years, and the modeling associated with this peril is much younger, with less than five years of material focus and investment. We can learn from the experience of the natural catastrophe modeling world, its evolution and interface with the insurance sector.

However, there are some key differences between the systemic risks of natural disasters and cyber events. One material contrast is that cyber perils manifest with active adversaries seeking to cause malicious damage to individuals and companies globally. The factors impacting modeling include the changing nature of geopolitical threats, the dramatic increase in the use of digital means for criminal enterprises, the hyperconnectivity of developed economies and an ever-increasing reliance on networked technologies.

The other challenge with modeling cyber-related perils is the limited volume of categorised and structured data relating to insured losses. There are many sources of well-documented cyber incidents, however, this has not translated into a similar volume of data from an insurance perspective. Similarly, there is a challenge in acquiring quality up-to-date information on company-specific cyber risk vulnerabilities and practices. Additionally immature data governance in a (still) emerging line of business has meant that individual causes of loss and individual sub-components of coverage have not been captured consistently or widely across the industry. This has made it harder to draw interpretations and insight for modeling purposes. Another challenge for modeling cyber risk is that many of the attacks which are being developed have never occurred previously, thus making it hard to measure their potential impact and severity.

By contrast, when modeling other phenomena such as pandemics, particularly notable given the crisis with the COVID-19 virus, there are separate challenges reflecting the interplay of human activity relating to transmissibility, as well as the contagiousness of the disease. There are significant instances of historical precedents to draw on as to how a disease may spread and manifest. This has a huge potential impact on both life insurance in terms of mortality rates, as well as health insurance relating to morbidity planning and management.

The Evolution of Cat Models

The devastating earthquake that struck San Francisco in April 1906 with a 7.9 magnitude, and the fire that followed was highly destructive. In terms of its impact, the then still small insurance industry was destroyed as the losses were over 100 times the amount of fire insurance premiums collected that year. The earthquake and following fire wiped out the profits of the preceding 47 years, leading to 14 insurers going out of business. Dynamite was used to level buildings in the path of the fire to create a fire break, which resulted in new fires and is believed to have caused more damage than it prevented, although buildings destroyed by dynamite were covered under property policies. One insurance issue which echoes through the decades into today's cyber insurance market is that each participating insurance company applied its own distinct policy terms and conditions in the case of the San Francisco 1906 quake. The inconsistency among clauses designed to limit fire liability resulting from an earthquake or building collapse proved to be particularly problematic in adjusting the losses on shared policies. There are distinct parallels in the way policy definitions are interpreted in cyber insurance policies today and specific exclusionary language used relating to triggers and types of business interruption losses.

There are significant lessons that can be learned from how the insurance market has addressed systemic risk and any variety of unexpected disasters – examples include the terrorist attacks of 9/11 and the Tohoku earthquake and tsunami that destroyed parts of Japan in 2011.

For example, Hurricane Andrew in 1992 was a human and economic tragedy that shocked the insurance industry resulting in 11 insurance companies closing down. The aftermath permanently altered the sector's approach to regulating, underwriting and managing catastrophe risk. The cyber insurance market has yet to experience a major catastrophic loss, but with lessons learned from the property insurance market, it can prepare for an event considered to be a case of not "if" but "when".

Hurricane Andrew highlighted the consequences of limited historic loss data and ushered in a new and increasingly sophisticated methodology for modeling extreme weather events to improve capital adequacy and economic stability. Analytical models based on data science and improved technology allowed for a new long-term view of potential catastrophe risk losses.

A report on the 20th anniversary of Hurricane Andrew examining its impact on the insurance industry by the Insurance Information Institute stated that "Insurers estimated the size of future losses using "experience" data based only on what happened in the past. Actuaries simply adjusted recent history to reflect current trends. However, [Hurricane Andrew] helped to prove that past data is a poor gauge for future catastrophe exposure. Previous projections failed to recognize that science indicated unprecedented events were within the realm of reasonable possibility." This statement applies to the world of cyber catastrophe risk management more today than ever, given the human threat element and the rapidly changing technology environment.

Cyber risk management is now benefiting from similar modeling approaches. Models provide a framework to inform these questions relative to the risk appetite of insurance companies and the industry in a rapidly changing threat landscape. Initially, individual scenarios were imagined that could represent systemic events to stress test the severity of impact on an insurance portfolio. This is known as "deterministic" modeling, or "conditional loss" modeling, which focuses on the severity of a given event, assuming that it has already happened, rather than trying to assess the likelihood of occurrence as well.

A probabilistic return period assessment for cyber risks is the next level of maturity, which addresses frequency as well as severity measurements. This approach includes a "Monte Carlo" simulation approach, which is a mathematical technique that generates random variables for modeling risk or uncertainty. The random variables or inputs are modelled on the basis of probability distributions. Many thousands of imagined simulated events are run through computer models using a random basis for generating different manifestations of these catastrophic scenarios creating a frequency estimation of occurrence. Insurance regulators are increasingly interested in models as a key part of cyber risk systemic exposure management.

How can cyber models be accurate given challenges with historic data?

For natural catastrophe risk models, using a historic view of risk from older data can be very meaningful. However, in the fast-changing world of cyber risk, it is much more difficult to utilise that data. For cyber risks, history is not a predictor of the future in terms of modeling as threat actors and the methods they deploy are constantly changing.

How can cyber models be accurate given challenges with historic data?

CyberCube examines historic data and the types of cyber incidents that have occurred although there are lots of challenges in the way that information is collected, curated and used. This historic data is used to understand better future potential systemic losses due to large-scale attacks on bigger and more interconnected entities. Adding in expert analysis on technology trends as well as the evolution and trends in targets, exploits, and threat actors allows Cybercube to develop cyber attack scenarios with a forward-looking view of risk.

We also look at other factors such as "outside-in" security data to understand better the network perimeter of an organization. This type of data captures information in a non-intrusive manner relating to specific security signals which can be identified from outside an organization. Examples include open ports, vulnerable hosts and end-of-life products. Additionally "inside-out" data from behind the firewall helps create a more holistic view of an organization's security. This data captures aggregated and anonymized "micro-segment" data about particular groups of companies. Taking that data right across a portfolio of companies and then applying them to scenarios where this type of systemic risk could manifest can create a meaningful forward-looking view of risk. This differs from natural catastrophe modeling (aside from recent climate models), which utilises an approach more akin to looking in the rearview mirror.

Defining a Major Cyber Event

One of the biggest challenges concerning cyber risk models centres around what constitutes a significant cyber loss. To date few events that have occurred are considered to have been significant enough to create a capital issue for the insurance industry. When modeling systemic cyber catastrophe risk, CyberCube considers scenarios that cross sectors and geographies. Unlike natural catastrophes, cyber risk can be regarded as geography agnostic.

Just as in natural catastrophe modeling, cyber risk models use multiple sources of data to derive an estimation of the frequency and severity outcomes of different events on a given insurance portfolio. Actuaries then measure and assess these to help set risk tolerance and capital requirements for the insurance industry. Scenarios are developed to represent a range of potential systemic events in which technological dependencies impact individual insured companies, due to a common vulnerability or a "single point of failure". Examples include common cloud service providers, payment systems, mobile phone networks, operating systems and other connected technologies.

Although cyber risk modelers do not have huge volumes of historical events to compare and draw insight from, there have been a number of events that, although perhaps not yet reaching industry catastrophe proportions, have nonetheless caused widespread technological impact, most notably the WannaCry ransomware attack and NotPetya event both in 2017. NotPetya originated in an attack on a widely-used Ukrainian tax software. It spread rapidly using a combination of existing malware, causing systems to be shut down due to a malicious code. Companies impacted most were those who had operations connected to those in Ukraine. Estimates of the economic impact range from $4 billion to over $8 billion and many household company names were impacted, including Maersk, Fedex, and Merck. Maersk alone has acknowledged a $300 million cost for the attack. The consensus is that the genesis of the attack was influenced by the Russian government, which has led to increased concerns around how to defend against hostile cyber activity.

Building a multi-dimensional picture of which factors will be most prominent and how they might manifest in systemic cyber loss is not easy. The cyber threat landscape is constantly evolving to bypass defenses, optimize itself for maximum damage and to increase the speed and scope of contagion. Those charged with predicting the size and shape of that risk – from within cybersecurity or insurance – face a major challenge in forming a forward-looking view of risk that applies multiple dimensions of data and insight to model possible outputs and identify trends before they become losses.

The "attack surface" across industries and system vulnerabilities is growing and increasingly interconnected, raising concerns around cascading impacts from a single major cyber event. The cyber attack field will continue to intensify, with more frequent, catastrophic attacks being met with a faster evolution of defense and cyber resiliency.

There are many pathways to a technologically feasible catastrophic event, although part of the challenge is developing scenarios, which, despite having no precedent, are both conceivable and viable given the active adversary threat landscape in which insurers operate. It is widely acknowledged that cyber catastrophes are something that should be planned for. The goal is to help the market prepare for such an event so as to avoid being blind-sided by a major and unanticipated loss.

As with any model, to cite a well-known phrase in statistical circles, "all models are wrong, but some are useful" (George Box). CyberCube does not have a predictive line of sight to the outcomes. There are limitations and assumptions in any model, especially relating to cyber risk, given the inherent uncertainties. However, these models provide valuable insights to better decision making relating to capital planning, reinsurance, and addressing regulatory issues. By learning from those difficult lessons of previous insurance shocks, we can support a more stable and resilient cyber risk insurance market.

Especially in cyber risk, history is not a predictor of the future, but we have the tools to learn from the past and enable informed decision making about capital management and balance sheet protection - fundamental issues for the continued stability and growth of the insurance industry and its clients. The good news is that these models are improving at a rapid pace with more useful data sources and faster cloud-based processing power. In embracing new and emerging risks, which is what the insurance industry has done for centuries, we can help reduce the uncertainty in planning for unknown risks. The insurance sector is better placed than ever to face the next challenge that arrives with the ever-changing technological and risk landscape.

Authors

Oliver Brew, Head of Client Services

Laurel Di Silvestro, Principal Client Services Manager

Yvette Essen, Head of Research & Communications

United States

CyberCube Analytics
58 Maiden Lane
3rd Floor
San Francisco CA94108

Email: info@cybcube.com

United Kingdom

CyberCube Analytics
51 Eastcheap
1st floor
London EC3M 1JP

Estonia

CyberCube Analytics
Metro Plaza
Viru Väljak 2
3rd floor
10111 Tallinn

CyberCube

www.cybcube.com