PUBLISHED AUGUST 2021

Cyber Risk Accumulation

CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

TThe American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Committee on Cyber Risk, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.

While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the committee.

American Academy of Actuaries

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

Cyber Risk Accumulation

Published August 2021

Accumulation risk in insurance, also known as aggregation risk, refers to the likelihood of a greater-than-anticipated accumulation of claim costs due to multiple exposures being tied to the same event or a related event. Our growing digital connectivity and interdependence mean that a single cyber event has the potential to simultaneously impact a significantly large number of businesses around the world.

For example, a rapidly increasing number of companies entrust their data and business operations to cloud services providers. The risk of disruption was realized in November 2020 when Amazon Web Services suffered an outage of undisclosed origin that took down a number of websites and online services.[1] Consequently, a successful cyberattack against a web service provider could translate into widespread business interruptions, or even the permanent loss of valuable data, depending on the severity of the attack. An insurance company or reinsurer exposed to such a cyber event—and an accumulation of claim liabilities—runs the risk of incurring extremely high aggregate portfolio losses.

Modeling accumulation risk is difficult because it can be challenging to identify the full set of dependencies among risks in a portfolio. Furthermore, traditional frequency/severity approaches are considered to be inadequate, or even unreliable, due to the lack of sufficient statistical data for new and emerging insurance lines. This is even more so for cyber insurance as the cyber breach targets and attack methods continuously evolve, and the bad actors continue to adapt and multiply.

Assessing accumulation risks requires transparency about digital supply chains and how commonly used software and systems can create systemic risk potential. Insurance consumers may not always understand their own cyber risk exposure sufficiently well to assemble and disclose the relevant data. And in a highly competitive insurance market, underwriters are often unable to obtain all of the key data points needed for the effective pricing of cyber risks. Fortunately, data such as company usage of information technology (IT) system components and malware propagation rates for devices, servers, and applications have become more available in recent years. While statistical data can be derived from past cyber incidents, historic events may be of limited use because of the rapid development of new threat vectors.[2] A recent example is the significant increase in working from home during the pandemic, which has made protection against cyber breaches more difficult and more complicated.

1 "Amazon Web Services outage causes issues for Roku, Adobe"; *CNBC*; Nov. 25, 2020.
2 Method or way a bad actor can breach or infiltrate an entire network/system. They enable hackers to exploit system vulnerabilities, including the human element.

Even with the availability of some data to model accumulation risk, cyber expertise is needed to piece together the useful data, apply judgment, and extrapolate what a tail event could look like. It is essential to evaluate the variety of commonalities among companies to identify non-obvious paths of aggregation. Cyber experts can help to understand the types of cyberattacks that are technically possible, the consequences of exploiting certain vulnerabilities, the motivations of different threat actor groups, the path a threat vector could take, and the plausibility that an adversary would attack a particular organization through a specific threat vector. Though reliance on cyber experts may be necessary when assessing accumulation risk, underwriters and actuaries would do well to remain abreast of cyber risk developments, including basic IT technology and terminology.

For decades, insurers have modeled accumulation risk from natural catastrophes, and some expect cyber accumulation modeling to mature in a similar manner. While both natural catastrophe and cyber accumulation modeling require blending data with expert opinion—and there can even be natural catastrophes, such as solar flares, that lead to insured cyber losses—cyber risk modeling presents many new challenges. Subject-matter experts strive to stay abreast of developments in the rapidly changing cyber landscape. Systemically important technology vendors can be the source of large-scale business interruption risk to global companies. Cyber damage is harder to quantify than property damage because the duration of a cyber event and reporting lag can vary significantly depending on the specific cyberattack. Sometimes a cyber breach, and the extent of the resulting damage, might not be known for months or more. Further, there is the possibility of underreporting of events as some organizations may be inhibited by the reputational damage from publicizing a significant breach or internal IT system/process failures.

Another distinguishing feature of cyber risks is that cyber catastrophes are typically man-made. An active adversary and motivational aspects of cyberattacks affect which entities are targeted. While people can be evacuated from the expected path of a hurricane to reduce the risk of harm, an active cyber adversary can adapt new tactics to cause damage that are not anticipated. Cyber catastrophic losses are also not isolated in confronting further risks. An earthquake in California may hardly influence expectations for the landfall of a hurricane in Florida, but a major cyberattack may expose new vulnerabilities, leading to further attacks.

To quantify cyber accumulation risk, a simple and conservative approach is to aggregate full insurance policy limits for the entire insurance portfolio. Beyond this, there are two main approaches to model accumulation: deterministic and probabilistic.

Deterministic accumulation modeling

A simple deterministic approach estimates potential losses using a third-party IT service provider's market share. For example, if a hypothetical Technology Provider A has a 20% market share, it can then be assumed that the firm has a roughly similar exposure to the universe of cyber threats. This means that 20% of the client companies in the insurer's well-diversified cyber portfolio would be at risk of experiencing a loss if Technology Provider A has a cyber event.

A more involved approach requires obtaining data on the technology providers (or at a minimum the primary ones) for each company in the insurer's cyber portfolio, taking care to identify those with higher limits. With specific data on which businesses are using which technology providers and other important information, exposures can be linked to aggregation points based on their particular technology providers. This approach can produce more accurate results because it relies on the detailed exposure data of entities in an insurer's portfolio instead of relying on broad industry statistics—but it requires significantly more effort and data to implement.

A possible basis on which to combine the two deterministic approaches would be to consider the mix of industries in one's portfolio and then make a separate assessment of the cyber threat level for each industry.

In both approaches, insurers will need to make deterministic assumptions for a cyber catastrophe scenario in order to assess its insured loss implications. For each cyber catastrophe scenario, estimates would be needed for the number of affected companies, the average costs per affected company, potential claim types triggered, and the available coverage per claim type. The total insured loss can then be calculated for each scenario.

Probabilistic accumulation modeling

In a probabilistic approach, losses are modeled using distributions instead of fixed averages to allow for variations in results. The market share approach can be expanded into a probabilistic model by assuming different technology provider market shares by industry and then creating a distribution of outcomes by repeatedly sampling across various segments of the insurer's portfolio. The process can be repeated for multiple technology providers. Correlation assumptions will be necessary to aggregate the potential losses.

The more complex form of probabilistic modeling is similar to some deterministic approaches, but the estimates made in each step need to be parameterized. The model begins with the creation of a catastrophic scenario narrative. The scenario needs to be realistic, relevant to the insurance market, and have some data available that can be used along with expert opinion to quantify its impacts. Examples of such scenarios include cloud provider outages, denial of service attacks, and mass data breaches. An annual probability of the catastrophic scenario occurring is estimated and assumed. Conditional on the scenario occurring, the next step is to estimate and assume the conditional probabilities of different severities. Finally, given both the annual probability and the severity probabilities, the last step is to determine the insurance cost of the cyber event. Probabilistic models like these have to be continually reviewed and revised based on changes in the cyber environment, including both the technological and legal aspects.

Emerging ideas

Much of the accumulation research to date has focused on an analysis of what potential attack scenarios might be encountered and assessing their likely impact. There are various models to help insurers manage affirmative cyber accumulation, but capabilities for non-affirmative (silent) cyber have been limited. Additionally, there is a gap in understanding the motivations of those behind these attacks. Technological vulnerability alone is not an adequate predictor of cyber risk, though the perennial risk of latent programming errors or compatibility issues cannot be ignored.

The manmade aspect of cyber risk is one of its fundamentally unique characteristics. Many businesses with state-of-the-art technology are breached while others with legacy technology have not been. Organizations with weaker security protocols and older IT operations are more likely to succumb to cyber events (e.g., spear-fishing and ransomware). Yet it is not clear whether they have been specifically targeted or whether they became one of many targets in an attack that was broadcasted widely. In this regard, cyber events could actually be much less random than they seem—in stark contrast to natural catastrophes. Studying the motivation of attackers could aid in looking at the problem.[3] Also, because cyber risks take place in a wide network of computers and systems, they could be modeled using interactive Markov chains or other network modeling techniques.[4]

3 "See No Evil, Hear No Evil? Dissecting the Impact of Online Hacker Forums"; *MIS Quarterly*; 2019.
4 "Pricing of Cyber Insurance Contracts in a Network Model"; *ASTIN Bulletin: The Journal of the IAA*; 2018.

Vendor models

Vendors providing cyber accumulation modeling services can be broadly grouped into two camps: traditional catastrophe insurance modelers expanding into cyber risks, and the typically newer cyber risk service providers moving into insurance. Generally speaking, the natural strengths and weaknesses of each type of vendor have become less pronounced as they are quickly learning from each other.

Many cyber accumulation model vendors were originally IT service providers, and they tend to have more in-house cyber expertise. Where data is sparse, expert judgment becomes increasingly important for assessing the next big emerging risk in the cyber domain, as well as staying on top of the dynamic landscape. Different models provide different degrees and types of flexibility in customizing parameters to reflect different views on cyber risk.

Due to data reporting requirements and data collection methods in the U.S., data may have a bias toward newsworthy, data breach events. Many cyber model vendors partner with others and incorporate multiple other data sources including outside-in scans (gathered from the public space), inside-out scans (gathered from an organization's internal network), threat monitoring (vulnerabilities on the surface, deep and dark webs), and firmographic data (company characteristics such as revenue and employee count).

Many vendors have built their databases though internal efforts and in partnership with others. Some vendors hire teams of "white hat" hackers to map out company networks and direct the types of data captured. Other creative methods include scraping online IT job ad requirements to make inferences about a particular organization's software and systems. The fact remains, however, that many small companies are still not included in these databases, and one may need to adopt a deterministic market share approach as a result. However, the small company databases are growing quickly as more vendors target small businesses in their initiatives.

At the March 2019 Cat Risk Management and Modelling conference held in London, the first public cyber model comparison exercise was completed.[5] Cyber model vendors were each provided with a common portfolio of 46 U.S. companies and a standard cyber insurance policy to model. The results of the models showed significant variation, indicating that the industry has not yet reached a consensus on accumulation modeling assumptions or its approach. As the industry matures, similar comparisons will likely continue to be

5 "Cyber Risk Models: Time for a Bench Test"; RMS, April 4, 2019.

performed for different cyber accumulation models. Additionally, given data challenges and the ongoing evolution of the nature of cyber risk, a vendor's model output may vary significantly from one version of its model to the next.

Accumulation modeling, and cyber risk modeling in general, are very active fields of endeavor and consequently subject to continual redevelopment and improvement. This means that the relative strengths and weaknesses of each vendor's products can be expected to shift and change over time. From an insurance writer's perspective, it may well be the case that no single vendor is able to completely capture cyber accumulation risk with a high degree of confidence. Inevitably, the cost to build and maintain models is a major factor to consider. Because of the difficulties that underlie accumulation risk modeling, managing the exposure may be as important as trying to accurately measure the risk.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**