Contents

A Guy Carpenter[1] and CyberCube Analytics[2] collaboration explores the size and shape of cyber catastrophes and the resulting financial impact on the U.S. cyber insurance industry.

Throughout this fluid process, models play a vital role in shaping the future state of cyber risk quantification. Tom Stone, Vice President of Catastrophe Modeling at CNA explained:

> "Cyber modeling doesn't yet have the currency of natural catastrophe models, so the industry is forced to dig in and understand how the models can be best leveraged to manage their risk."

A growing and maturing market demands additional sophistication via a data-driven approach to understanding the potential impact of catastrophic events.

Cyber risk in a catastrophe context: Terrorism case study

The evolution of the market

The terrorism market has been reactionary to major loss events, for example, the IRA bombings in the United Kingdom and the terrorist attacks of September 11, 2001 in the United States. The cyber market can also be reactionary, particularly concerning some of the earlier years of breach losses, but cyber has been comparatively more proactive as an evolving product.

The terrorist attacks of September 11, 2001, as an event were far beyond the expectations generated from any previous view of terrorism risk, and caused a necessary market adjustment. A number of insurance lines absorbed costs during the terrorist attacks of September 11, 2001 in a manner that was exacerbated by coverage uncertainties. The market has since matured and there is now a clearer sense of where the terrorism market lies. This maturing of the terrorism market provides an ideal case study for the cyber market's current challenges relating to affirmative, silent and non-affirmative coverages.

The challenges of modeling

The challenges of modeling cyber are well-known. These include the lack of event data, expansions of coverage and uncertainty as to the appropriateness of historic experience to project forward a prospective view, and what constitutes "limiting factors" for a cyber event.

Considering terrorism risk in terms of probability and consequence, probability is assessed in terms of intent and capability, which can help set a framework for quantification, and intent and capability to conduct conventional terrorism or cyber-terrorism can be (but are not necessarily) related. There are parallels here that can be drawn in the deployment of the corresponding "kill chain" methodologies used in both fields.

Data collection for terrorism events is not perfect, but it does represent a benchmark to aspire to, with the presence of such initiatives as the Global Terrorism Database. Certain risks will be modeled based on events that have occurred up to that time. This is a lesson that the terrorism market has had to learn through some of its key historic events.

More recent micro terrorism incidents have again shifted this view, with events such as the Nice, Paris Bataclan and London Borough Market attacks having had a significant human impact but without the same property damage associated with earlier generations of terrorism attacks. It is important that modeling is not "static" between incidents and that it engages creatively and proactively in identifying new and emerging scenario types.

Many of the challenges of modeling terrorism bear similarities to that for cyber. The current generation of cyber models needs to grapple with these challenges of presenting this same full spectrum view. This requires that we learn the lessons of

Don’t look back

Although future loss estimates can be a subject of debate, there is consistency with the scale of financial impacts as a result of cyber events, regardless of line of business:

What is a “Single Point of Failure”?

CyberCube’s Portfolio Manager combines enterprise data for millions of companies worldwide, with flexibility built in to augment or adjust key parameters of enterprise data.

These include:

- Organizational footprint: assessed against factors internal and external to the enterprise, enabling a comprehensive

Scenario Narratives

Key takeaways from the analysis of the various scenarios:

1. The costliest cyber catastrophe scenario modeled was *widespread data loss due to zero-day vulnerabilities within a leading operating system*, causing a USD 23.8 billion insured loss. The likelihood of this scenario is the lowest (beyond the 1:300 year return period), but it produces the greatest size of loss. This event is similar to what happened with the NotPetya attack. A zero-day vulnerability is a flaw in software or hardware that the developer has not had an opportunity to patch. These enable attacks that are potentially not covered by existing cyber defenses.
2. The most likely cyber catastrophe loss scenario is *widespread data theft from a major email service provider. Large-scale ransomware at a leading cloud services provider* is the second most likely scenario.
3. On an industry basis, financial firms are most impacted during these systemic events, with at

For the (re)insurance industry, the importance of understanding

I. Long-lasting outage at a leading cloud service provider

The model showed that a long-lasting outage from a leading cloud service provider could trigger an insured loss of **USD 14.3 billion**. The outage time in this scenario ranges on a scale of days to weeks, depending on the redundancies and resiliencies of individual companies.

A major cloud service provider with significant market share operates globally with many regional hubs and data centers in the United States and other hubs worldwide, to serve its international client base. In this scenario, a disgruntled employee of this cloud service provider releases malware. The primary goal is to compromise targeted system availability for as long as possible, triggering short-term economic losses and diminishing confidence in cloud solutions. The malware then infects the system and causes a service outage and ensuing business interruption.

Cost components

By far the largest component of the insured loss would be BI costs of USD 13.1 billion – 92 percent of the entire insurance cost related to the incident.

Considerations for insurers

Cloud adoption is highest in larger companies, which are increasingly migrating critical business systems to the cloud.

II. Large-scale cloud ransomware at a leading cloud services provider

A large-scale ransomware attack at a leading cloud services provider would trigger insured losses of **USD 11.5 billion**

losses. This is an artificial distinction; implicitly, it does not recognize the fact that one scenario characterizes an attack vector and the other relates to a disruption of a systemically-significant target. One of the scenarios modeled in this exercise set out how the vector and target can conceivably be combined into one scenario strand. This is not a purely

III. Widespread data loss from a leading operating system provider

A widespread data loss from this SPOF could result in a systemic event amounting to **USD 23.8 billion** in insured losses. While this is the largest loss modeled, the frequency of this event is among the lowest of the scenarios in this report.

Cyber criminals find and exploit a vulnerability in a popular operating system. The primary goal is to disrupt all computers running this operating system in an effort to achieve fame, triggering short-term economic losses and showcasing the technical capability of the attackers. Data from hard drives of all infected computers is lost.

Cost components

IV. Widespread theft from major email service provider

A widespread theft from a major email service provider would trigger insured losses of **USD 19.1 billion.**

In this scenario, a phishing campaign consisting of conventional and more advanced phishing techniques infects enterprise email clients with malware, affecting a significant proportion of all accounts. The primary goal is to steal and monetize login credentials and personally-identifiable information (PII). This leads to the attackers profiting from the sale of records, further identifying more valuable assets in corporate managed email accounts such as intellectual property, and showcasing their hacking skills.

Cost components

Most of the loss from this type of cyber attack would involve confidential information, intellectual property and PII.

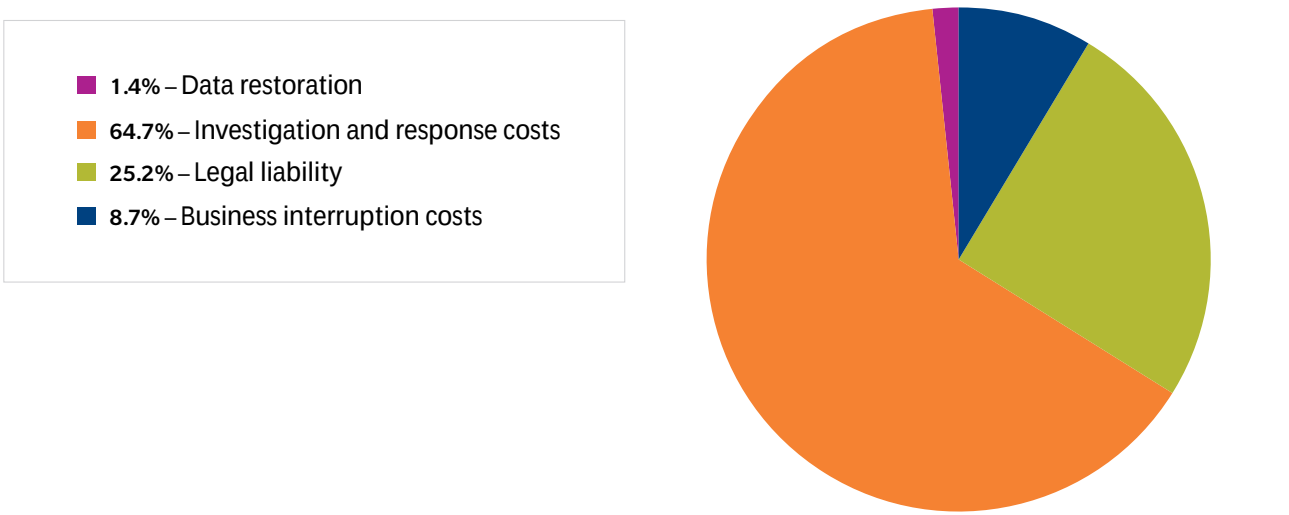
The main drivers of insured loss here are investigation costs and response costs (64.7 percent), followed by legal liability (25.2 percent). Business interruption is a minor component of this scenario, at just USD 1.7 billion (8.7 percent).

Considerations for insurers

Data breach has historically been the driver of claims under standalone cyber insurance policies. This scenario-based study demonstrated the potential impact of a variety of as-yet-unrealized events on coverage areas such as business interruption.

However, data breach and the associated costs of remediation remain significant cost drivers in this synthetic U.S. industry portfolio.

FIGURE 6. Wide p□ead Da a Thef a Leading Email Se□ ice P□o ide□b Co Componen



Source: Guy Carpenter & CyberCube Analytics

V. Large-scale data loss from leading service provider

If there were a large-scale data loss at a leading cloud service provider, the model predicts insured losses of **USD 22.2 billion**.

In this scenario, a threat actor obtains access to a data center by targeting the support staff, and then uses the compromised staff credentials to spread through the network and gain escalated remote access. The primary goal is to permanently erase cloud services customers' instances and stored databases to create disruption and chaos. The attacker executes commands to the system that are either hard to detect or are irreversible, triggering permanent economic losses and showcasing the attackers' technical capability.

Cost components

In a long-lasting outage at a leading cloud service provider and data loss at a leading operating systems provider, BI costs feature heavily for a large-scale data loss in this scenario.

Conclusion

Our examination of the key drivers of catastrophic insured loss within the U.S. cyber insurance market and how these results can be incorporated into portfolio construction, risk retention and transfer strategies and capital allocation was designed to contribute to important conversations around:

- Developing portfolio strategy
  - Pricing: understanding the components of loss ratios and catastrophe loads
  - Limit/attachment profiles: how do they inform portfolio construction?
- Exposure management and reinsurance
  - Buying reinsurance: structuring programs and setting appropriate limits
  - Understanding tail risk: how does this inform accumulation risk?
- Capital allocation and realistic disaster scenario planning
  - How does cyber feature in capital allocation decisions?
  - At a group level, how does this information shape our cyber growth strategy?
  - How can models help develop strategy and test assumptions?

Appendix

The industry loss estimates that we examine in this report are not predictions and should not be used as the sole basis of cyber risk strategies. The study was aimed at highlighting particular vulnerabilities that can be exploited to execute a cyber attack and exploring the volatility around frequency and severity of those attacks. Analyses such as this one are useful in examining the multiple views of cyber risk, catastrophe potential and the factors shaping the continued growth of the cyber insurance product.

Given that the scope of the study was U.S. standalone cyber policies, the loss estimates in this report are not a proxy for cyber catastrophe loss quanta across the globe. Nor do they represent losses arising under package policies and non-affirmative cyber coverage.

In addition, the study looked at the industry as a whole. However, this masks the fact that individual carriers with different policy wordings; different portfolios of companies, for example, industry mix and company size; and different underwriting strategies, will have very different losses from these catastrophic events. To understand the impact of these scenarios on a particular book of business, modeling needs to be run on that book of business.

Study methodology: CyberCube Portfolio Manager

CyberCube has access to data from both inside and outside the firewall, building a uniquely forward-looking view of risk. Exclusive access to telemetry from the world's largest cybersecurity firm, Symantec – and other data partners – equips (re)insurers and brokers to see trends before they become claims.

In addition, CyberCube's deep bench of cybersecurity and insurance experts select the best sources of data and turn them into early indicators of risk that decision-makers can trust.

The team is composed of multi-disciplinary professionals across data science, cyber security, artificial intelligence, software engineering, actuarial modeling and commercial insurance.

CyberCube was founded as an independent company in 2018, with backing from ForgePoint Capital. Starting in 2015, the team benefited from more than two years' focused research and development within Symantec, which continues to be a key strategic partner.

For the purposes of this study, Guy Carpenter applied

CyberCube has developed a data schema that is simple to use yet has the power to drive detailed outputs.

The **scenario catalog** comprises a broad spectrum of threats and exposures. Scenario classes were designed in consultation with (re)insurers and cyber security experts, taking into account regulatory priorities for scenario development. The classes represent the most significant sources of risk accumulation arising from "catastrophe" scale events. There is a program of continual research and consultation to inform further development of the scenario catalog.

The **probability** component is powered by a range of techniques to combine estimates from different sources. This thorough approach is essential in forming probabilities for events that are subject to great uncertainty and for which there may be no historical precedent. Only through major investment in gathering and assessing multiple high-quality data sources is the model able to derive probability estimates that are defensible and useful.

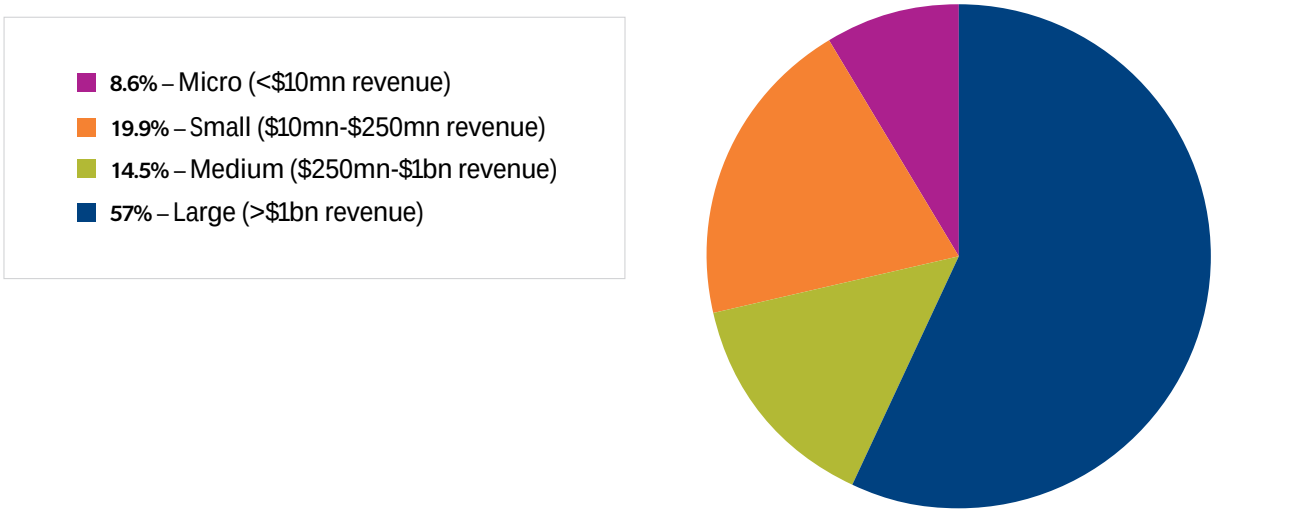
The **footprint** of a catastrophic cyber event relies on assessing the systemic connections of shared technology dependencies. CyberCube has mapped more than 1,000 strategic software and services to identify specific dependencies within their enterprise dataset. This reveals the systemic effects of catastrophic cyber attacks, allowing the identification

Study Methodology: Guy Carpenter's synthetic portfolio

Guy Carpenter started with a base portfolio of just over 6,000 cyber insurance policies with a combined premium of USD 285 million. This base portfolio was estimated to represent about 10

Unless otherwise stated, the figures quoted in this report are the Aggregate Exceedance Probability.

FIGURE 8. Portfolio Premium by Size of Business



Source: Guy Carpenter & CyberCube Analytics

Assessing the modeled portfolio by industry category, the largest single industry that contributed to portfolio premiums was Information Technology (USD 641 million), followed by Financials (USD 398 million). Retail companies generated a total premium of USD 313 million to come in third. These industries are large buyers of risk transfer and would be expected to contribute most to the portfolio premiums.

GUY CARPENTER

About Guy Carpenter

Guy Carpenter & Company, LLC is a global leader in providing risk and reinsurance intermediary services. With over 60 offices

MARSH & McLENNAN COMPANIES