GUY CARPENTER

CyberCube

A U.S. Cyber Insurance Industry
Catastrophe Loss Study: 2019

# Looking Beyond the Clouds

MARSH & McLENNAN COMPANIES

# 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.



1. Guy Carpenter & Company, a wholly-owned subsidiary of Marsh & McLennan Companies Inc.
2. A ForgePoint Capital portfolio company

# Executive Summary

The inexorable spread of the digital economy is fundamentally changing the nature of risk, presenting unique opportunities – and challenges – to the (re)insurance industry. How the industry responds to the rapid pace of technological change is crucial to its long-term relevance and growth.

The constantly evolving nature of cyber risk makes it challenging to definitively quantify, yet it is critical for (re)insurers to understand the impact of severe events to inform strategy and risk tolerance. It is essential to develop a deep understanding of the characteristics of cyber catastrophe events and the financial impact they could have on the standalone cyber insurance market today. As the (re)insurance industry seeks to reduce protection gaps and drive cyber product adoption, the future growth that results will help develop a robust market better equipped to absorb the potential for large-scale losses.

With that premise in mind, CyberCube Analytics and Guy Carpenter collaborated on an endeavor to help (re)insurers quantify cyber risk by pooling data resources and analytics capabilities in order to cultivate a view of the potential U.S. cyber industry loss from among a range of cyber catastrophe scenarios. CyberCube offers a software-as-a-service analytics platform for cyber risk aggregation modeling and insurance underwriting. The study aims to contribute to the discussion surrounding 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.

## The study highlights five key considerations for (re)insurers and other stakeholders to help protect profitability and examine capital adequacy of the existing U.S. cyber standalone insurance industry.

- The U.S. industry 1-in-100 year return period produces total annual cyber catastrophe insured losses of USD 14.6 billion (this can include one or more events within the same year).
- Both on-premise and cloud service providers face exogenous threats from malicious third parties. Focusing on cloud service providers, the calculated probability of ransomware is four times larger than the probability of other outages.
- The top five scenario classes comprise roughly 75 percent of the total average annual loss (AAL).
- The costliest cyber catastrophe scenario is widespread data loss from a leading operating systems provider with potential to generate up to USD 23.8 billion of insured loss.
- The most likely cyber catastrophe loss scenario is widespread data theft from a major email service provider.

Although standalone cyber insurance (excluding surplus lines policies, endorsements, sub-limits, package policies and non-affirmative cyber in other insurance lines) has experienced favorable loss ratios to date, the global economy has yet to experience a systemic, sustained cyber event that creates disruption and financial loss on a scale that causes an earnings or capital event for the (re)insurance industry.

The closest such events were NotPetya and WannaCry, which in 2017, caused widespread disruption – with economic losses from NotPetya estimated as high as USD 10 billion. The insurable impact, however, was muted due to many of the compromised businesses being underinsured or not purchasing a cyber insurance product. As the cyber market continues to develop, the industry must be increasingly positioned to understand and sustain such potential events.

With very little precedent, (re)insurance carriers are challenged in estimating the size and scope of a catastrophic cyber event on their balance sheets. Yet, this catastrophic component adds complexity and considerable risk in both typical and worst-case years that must be contemplated in forming robust and reliable growth strategies for this line of business. This process is as much of an art as it is a science. As stated by Rory Egan, Senior Cyber Actuary with Munich Re:

"The fundamental first step towards quantifying the catastrophic potential from cyber risk is to identify which sources of risk are currently manageable by the cyber (re) insurance market, and which can and should be modeled, versus those which cannot. Ultimately we, as a market, should aim to provide meaningful risk transfer mechanisms but these need to be sustainable. Therefore it is important to dedicate significant expertise and effort towards ensuring a solid scientific basis underpinning risk appetite and modeling approaches, in order to provide such solutions."

In the study, we analyzed all 23 catastrophe loss scenarios on CyberCube's platform, which range from attacks on critical infrastructure to third-party technology aggregation scenarios to attacks that affect the cloud environment.

We focused on the five that drive the highest loss values. For each, we considered the size of the loss, the single point of failure (SPOF) targeted to execute the attack and the implications of these findings on the insurance market.

The five major contributing catastrophe scenarios are:

- Long-lasting outage at a leading cloud service provider (USD 14.3 billion loss)
- Large-scale cloud ransomware at a leading cloud services provider (USD 11.5 billion loss)
- Widespread data loss from a leading operating system provider (USD 23.8 billion loss)
- Widespread theft from major e-mail service provider (USD 19.1 billion loss)
- Large-scale data loss from cloud service provider (USD 22.2 billion loss)

Across the 23 scenarios considered in the research for this study, the largest loss cost contributor was business interruption – with the scenario of *widespread data loss due to a vulnerability within a leading operating system* ranked in the top three to four for both AAL and maximum loss. Cloud outage and data loss are also significant events in driving loss costs.

Insurance companies and the organizations they insure need to be aware of these major catastrophic scenarios, and understand the response plans necessary and potential financial losses in each. Bearing this in mind, the industry must invest in effectively assessing and managing aggregations, educating the business community to drive product adoption, and quantifying cyber risk to promote the purchase of adequate insurance limits.

By understanding risk tolerance and capital commitment, primary carriers can also ensure that they have purchased enough reinsurance capacity in a structure that best protects against these events. Andy Lea, Vice President of Underwriting for Cyber, Error & Omissions and Media at CNA said:

"Cyber threats are omnipresent; businesses' ongoing reliance on ever-more-complex technology solutions makes that inevitable. Modeling for cyber is still in its early days, and most insurance companies are trying to better understand how current efforts reflect the aggregate risk of a cyber event impacting hundreds or even thousands of insureds at the same time, and what that in turn means for our own enterprise risk management efforts."

We explored the study's findings in the context of helping (re) insurers investigate portfolio construction, risk retention and transfer tactics, capital allocation – and how robust modeling and analytics can inform these strategies.

## Growing pains: The catalyst for this study

According to some estimates,[3] the global market volume for cyber insurance will grow to USD 8 to 9 billion by 2020 – more than twice that of 2017. With many traditional lines of insurance experiencing stagnating growth, cyber is increasingly viewed as having large growth potential for commercial property and casualty (re)insurers.

Despite this growth potential, there are headwinds to overcome as cyber insurance continues to grow and evolve. Increasing competition as new entrants seek to take advantage of the growth potential has created pressure on rates as well as an expansion of available coverage. The exposure data needed by (re)insurers to quantify and price cyber risk appropriately is a moving target as coverage matures and (re)insurers develop a deeper understanding of how to translate cybersecurity metrics into indicators of loss.

3. https://www.munichre.com/en/media-relations/publications/press-releases/2018/2018-10-22-press-release/index.html

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.

To enable the industry-wide analysis, the researchers constructed a synthetic USD 2.6 billion portfolio using anonymized cyber insurance policy characteristics. They built the portfolio by extrapolating from these characteristics to create an amalgamation of risks representative of the standalone U.S. cyber insurance market. In the next step, they stress-tested the portfolio using a number of cyber catastrophe scenarios on CyberCube's analytics platform.

The study reflected the impact of catastrophic losses on an *insured* portfolio. Catastrophic loss is defined as a cybersecurity failure at a SPOF causing losses to occur at many other companies. The severity of the losses discovered in this research was based on the insurance limits purchased by the insured entities. The study's intent was to provide a realistic reflection of the potential losses that the U.S. cyber insurance market could face today rather than on economic losses or estimates of possible application of non-affirmative cover.

## Modeling Parallels

Modeling cyber risk has unique complexities. Natural catastrophe modeling has existed for more than three decades but it is still not error-free. Cyber catastrophe loss modeling, being a new discipline, faces challenges similar to those of natural catastrophe modeling in addition to tackling an amorphous risk with little relevant historical data and a rapidly changing nature. Andrew Kwon, Lead Cyber Actuary for Zurich, concurred:

"Extending the lessons learned from property cats to the cyber space is intuitive and logical, but cyber continues to be a unique force unto itself. A hurricane does not evolve to bypass defenses; an earthquake does not optimize itself for maximum damage. However, cyber does face those challenges. Managing return on capital requires continued development of innovations in data, modeling, tactics and strategies – to comprehend what we have seen, and to prepare for what is yet to come."

With natural catastrophes, the flooding of a semi-conductor factory in Thailand does not mean a factory in the United States is any more or less likely to flood. Cyber aggregation events are not necessarily discrete attacks that affect only limited geographies or individual insureds.

It is interesting to compare cyber risk modeling to that of terrorism modeling – a discipline that has developed in recent years to address a malicious, man-made peril. See the Terrorism section on page 9.

Cyber risk's unique characteristics prompted this ground-breaking study. The challenge we address is how to take a forward-looking view of cyber catastrophe risk to enable controlled and profitable growth of the insurance industry.

The synthetic portfolio that Guy Carpenter created (see *Appendix* for additional detail) was broadly representative of the U.S. standalone cyber insurance market. As the market-leading cyber reinsurance broker, Guy Carpenter is uniquely positioned to apply its knowledge of the market landscape to create a synthetic portfolio.

CyberCube has access to security data from both inside and outside the firewall, with exclusive access to telemetry from cybersecurity firm, Symantec – and other data partners. This data and additional analytics allowed CyberCube to create realistic catastrophe scenario narratives and apply frequencies and severities to them to build a probabilistic model.

# 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 experience while seeking to identify and quantify emerging risks.

## Don't look back

The modeled U.S. industry **1-in-100** year catastrophe loss from a cyber event is estimated to be

**USD 14.6 billion**

The modeled **1-in-200** year catastrophe loss is estimated at

**USD 16.1 billion**

of insured loss.

The cyber insurance market has grown, and grown profitably for the industry for the last several years – though some could argue those results may be misleading. Available loss information is predominantly non-systemic in nature, which comprises the vast majority of the cyber insurance industry loss ratio to date. Among the limited losses related to systemic events, the threat landscape is dynamic, creating challenges in drawing conclusions from these limited datasets. Rory Egan (Munich Re) acknowledged these difficulties, stating:

"The underlying risk changes as technology and legal frameworks evolve, and the market evolves with it through updated cyber policy design. So when quantifying potential losses at extreme return periods, approaches based on historical experience are inadequate. Further, the industry has not yet reached a consensus on the appropriate 'event set' for cyber risk that should form a holistic cyber risk accumulation risk management framework. Therefore, we conduct forward-looking analyses of the threat landscape, with some key questions in mind: Who are the different threat actors out there? What are their capabilities and objectives? What are the critical components of information technology infrastructure and what vulnerabilities exist that could be exploited, resulting in impacts felt across many organizations and individuals?"

Historically, cyber insurers have seen a series of one-off data breach losses, some of which – the Marriott data breach in 2018, for example, with breach costs estimated at more than USD 2 billion[4] – are not fully captured by industry loss performance, since the insurance limit purchased was far less than the expected ultimate economic loss.

The largest multi-insured loss arising from a cyber attack is the NotPetya event in 2017, estimated by Property Claim Services (PCS) at more than USD 3 billion.[5] However, due to underinsurance and low product penetration by the affected businesses, most of that loss will likely fall to the non-affirmative insurance market, and claims under non-affirmative policies are being contested by some carriers. Due to the business community's growing interconnectivity and increasing reliance on technology, cyber losses will continue to manifest in new and unexpected ways. The protection gap disparity highlighted by NotPetya between economic and insured loss may be only a sampling of what is to come.

4. https://www.jlt.com/en-dk/insurance-risk/cyber-insurance/insights/marriott-breach-to-test-insurance-response
5. https://www.artemis.bm/news/merck-silent-cyber-impacts-drove-petya-industry-loss-pcs/

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:

- Cyber crime costs are predicted to hit USD 6 trillion annually by 2021. This followed a record year in 2017 of USD 600 billion.[6]
- The World Economic Forum's 2019 cyber crime estimates[7] put economic losses from cyber crime at USD 3 trillion by 2020.
- In the "Bashe Attack: global infection by contagious malware 2019," the global economy is described as underprepared, with 86 percent of the total economic losses uninsured, leaving an estimated insurance gap of USD 166 billion."[8]

To help the (re)insurance industry sustain the full potential impact of these economic losses, the cyber market must further develop by increasing buyer penetration, assisting businesses in understanding and quantifying their cyber exposures and continuing to prudently expand the product so that it bridges cyber protection gaps across lines of business.

A large privacy breach such as Marriott or a systemic malware event is a future scenario that (re)insurers need to understand and account for, but adequately doing so requires growing the product space in a way that closes the gap between insured and economic loss sums. Addressing the issue of modeling cyber catastrophes to better price these scenarios into insurance products is key to creating a sustainable solution and adequate capacity for insurance buyers and the (re)insurance value chain.

The (re)insurance market is still in learning and growth mode, as evidenced by the inconsistent views of cyber risk, particularly at the catastrophic level. The results of this study highlighted the need for insureds, insurers and reinsurers to all recognize the loss potential of cyber catastrophes, and the value in appropriately priced risk transfer solutions. Kelly Bellitti, FCAS and Head of Global Cyber Pricing at AXA XL, recognized these hurdles, saying:

"It is a challenge to estimate cyber cat loads given both the lack of historical industry events and the rapidly evolving nature of cyber risk. There are many companies out there creating solutions to help the (re) insurance industry address this problem. Utilizing a multi-dimensional approach allows us to review many different views of our cyber risk, quantify our exposures and manage accumulations."

## Vulnerabilities...

Key SPOFs that could lead to the costliest losses include: operating systems providers, email service providers, cloud service providers and critical utilities providers.

Many cyber underwriters consider the cloud to be a major SPOF in causing a systemic cyber attack. Adoption of the cloud for business use is certainly increasing dramatically. A LogicMonitor survey in 2018 suggested that 83 percent of companies will be using the cloud by 2020.[9] There is less understanding within the insurance industry of the implications of cloud services. The cloud is not one service, but rather several different types of service – storage, computational power, back up services and so on – and the dependencies on these vary.

However, our study found that major cloud service providers are just one class of SPOF generating catastrophe loss. As we explore in the next section, other SPOFs that should be considered include operating systems providers, email servers and critical infrastructure providers, because these also serve as points of aggregation, thus enabling a systemic loss in the event of cybersecurity failure.

6. "Economic Impact of Cybercrime — No Slowing Down," McAfee and the Center for Strategic and International Studies (CSIS)
7. https://www.weforum.org/agenda/2019/05/helping-small-businesses-fight-cybercrime-benefits-the-global-ecosystem/
8. https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/bashe-attack
9. https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/

# 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.

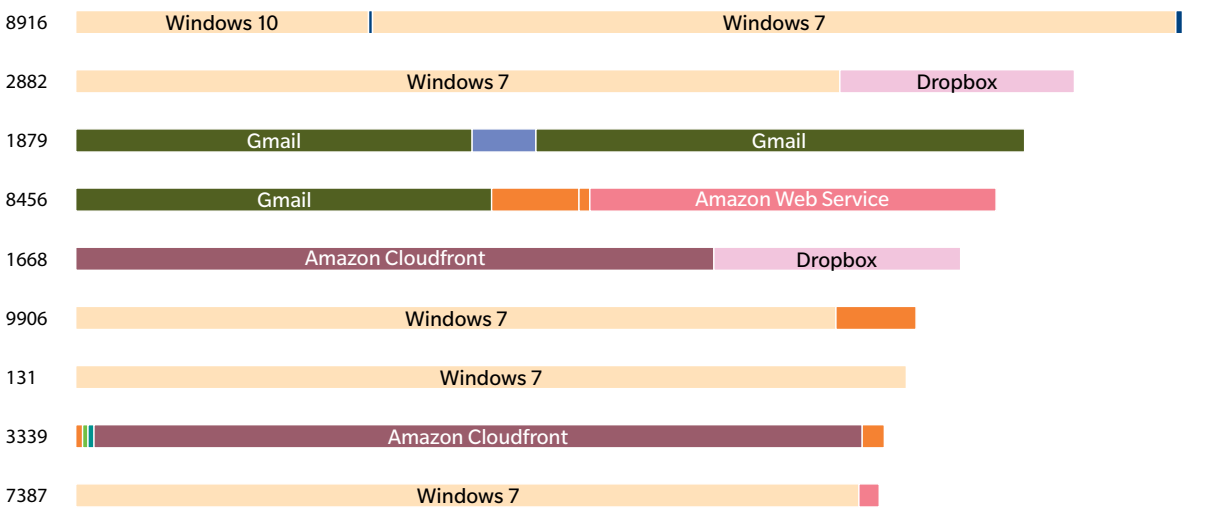
These include:

- Organizational footprint: assessed against factors internal and external to the enterprise, enabling a comprehensive view of key technology dependencies and the "attack surface" available to malicious actors.
- Organizational attractiveness: measuring a range of assets and characteristics that could provide a motive for any class of threat actor to target the enterprise.
- Cyber vulnerabilities: derived from analysis of internal and external telemetry. This holistic view enables measurement of the relative success rate of cyber attacks.
- Cyber security posture: measured against a wide range of indicators that provide insight on the quality of security in place.

Across the millions of companies analyzed in this way, a few key technology dependencies recur and manifest as potential vectors for a widespread cyber attack on multiple companies across multiple geographies at one time. CyberCube calls these Single Points of Failure (SPOFs).

The Portfolio Manager generates output such as the chart below, which breaks down the SPOFs driving tail results within the modeled portfolio. For each simulated year (out of the 10,000 total), this output shows the years ranked from highest to lowest by total annual loss, and the SPOF behind an event. The x-axis is the loss dollar amount. For example, in Simulation Year 2882, two events occurred, one resulting in data loss from a common operating system (Windows 7), and a second event where Dropbox was affected by a large-scale ransomware attack.

**Figure 1. Results by Simulation Year**




*Source: Guy Carpenter & CyberCube Analytics*


mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
elif operation == "MIRROR_Z
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
print("please select exa
OPERATOR CLASSES
# Mirror Tool

# 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 least 20 percent of the insured loss overall. The accumulation of insured loss among financial firms is reflective of the buying patterns of this sector, with large banks and other financial firms driving some of the highest adoption rates of any industry sector. These companies also represent lucrative targets and therefore attract greater attention and loss potential.
4. Companies with revenues greater than USD 1 billion, regardless of industry sector, represent roughly 75 percent of the insured loss.
5. While the cost components of each of these scenarios vary, it is notable that business interruption (BI) costs, caused when supply chains stall or factories are offline, feature heavily in the catastrophe costs. The BI components of cyber insurance have evolved rapidly in the last few years, and the take-up by purchasers has increased as the awareness of the criticality of systems has grown. The low-frequency and high-severity aspects of catastrophic BI events affirm this improving understanding of these exposures.
6. Fines and penalties currently represent a small proportion of the cost component of the five scenarios addressed in the report. However, the European regulators recently imposed large General Data Protection Regulation-related fines on British Airways (USD 230 million) and Marriott International (USD 124 million), and in the United States, the Federal Trade Commission imposed a USD 5 billion privacy-related fine on Facebook. Going forward, the relative importance of fines and penalties as cost components in a systemic attack may be set to change.

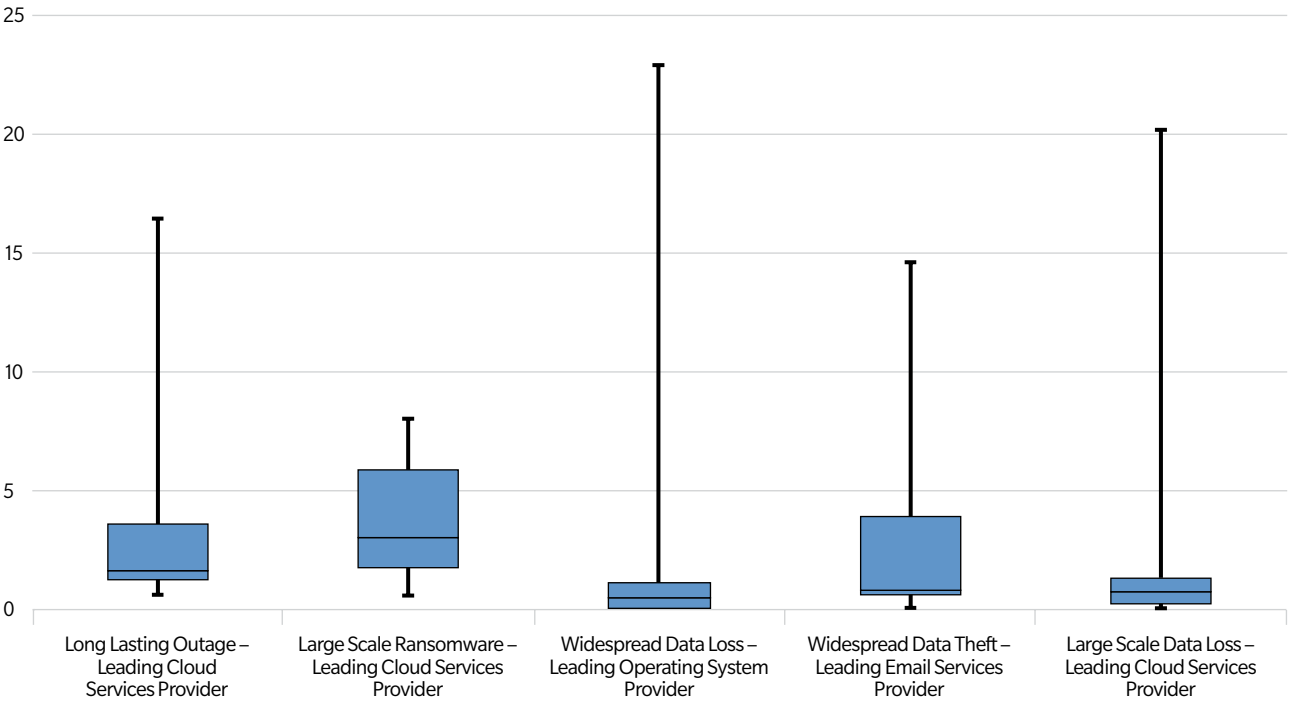
For the (re)insurance industry, the importance of understanding these scenarios is that it enables insurers to allocate capital appropriately and develop more nuanced underwriting strategies that take into account the type of events that could impact a portfolio.

Carriers can also use these scenarios to compare risk appetite across lines of business to ensure that they have purchased enough reinsurance capacity in a structure that best protects against these events.

Lastly, by having an understanding of catastrophic cyber scenarios, underwriters can set risk appetite, inform portfolio strategies and determine how they deploy capacity to cyber risks.

Figure 2 shows the possible range of loss severity and volatility over 10,000 simulated years for the five most impactful scenarios from the 23 available scenarios in the CyberCube model, covering a range of possible attack vectors and SPOFs. We consider each of the major contributing scenarios in turn here.

**Figure 2. Conditional Loss Distribution by Scenario: Top 5 (USD Billions)**




*Source: Guy Carpenter & CyberCube Analytics*

By having an understanding of catastrophic cyber scenarios, underwriters can set risk appetite, inform portfolio strategies and determine how they deploy capacity to cyber risks

# 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.

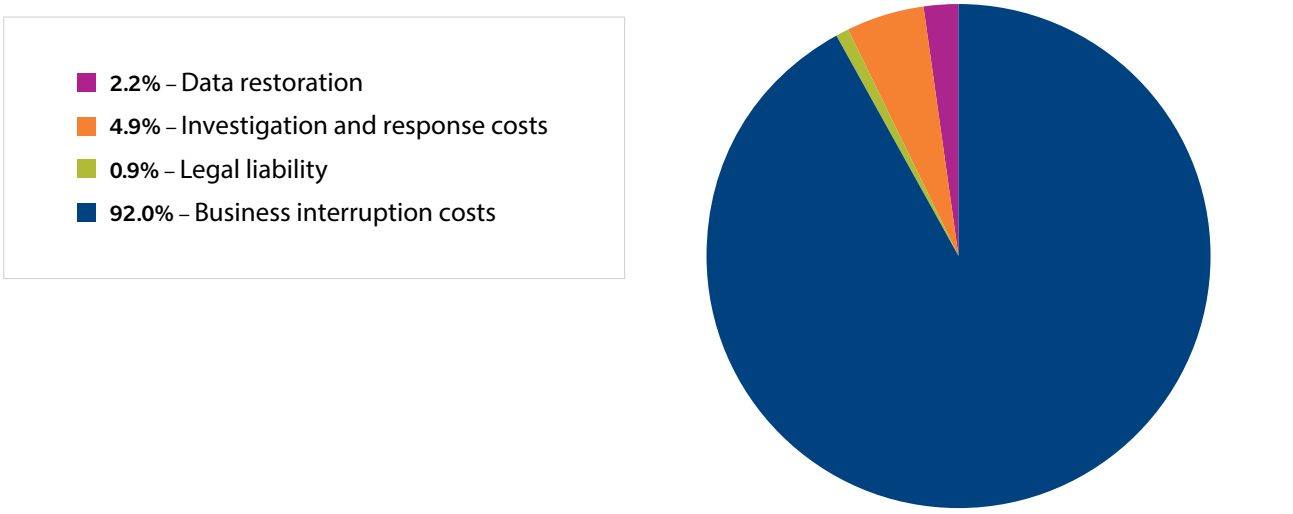
## Cost components

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. It is also noteworthy that different industry sectors have adopted cloud-based computing at different rates. Consequently, this has potential implications for the impact of a cloud outage. The dominance of BI losses in this scenario indicates that industrial control systems, just-in-time supply chain management and critical customer interfaces are increasingly reliant on cloud technology and should be considered when analyzing potential insureds.

Figure 3. **Long-lasting Outage at Cloud Service Provider by Cost Component**




*Source: Guy Carpenter & CyberCube Analytics*

# II. Large-scale cloud ransomware at a leading cloud service provider

A large-scale ransomware attack at a leading cloud service provider would trigger insured losses of **USD 11.5 billion**. The range of losses for this scenario is narrower than for others. However, due to the frequency of this event, it is ranked among the top in terms of contribution to the mean loss. This underlines the importance of a catastrophe load that factors in both frequency and severity.

A group of cyber criminals targets a major cloud data storage company and encrypts all data using malware. The primary goal is to get the company to pay a ransom in exchange for the attackers providing decryption keys to unlock critical data, triggering short-term economic losses and showcasing the technical capability of the attackers.

During the attack, all data stored on the cloud is locked, which may take days, if not weeks or more, to be restored. In some extreme cases, some data may be permanently lost. System shutdown leads to losses from business interruption/contingent business interruption and massive operational disruptions.

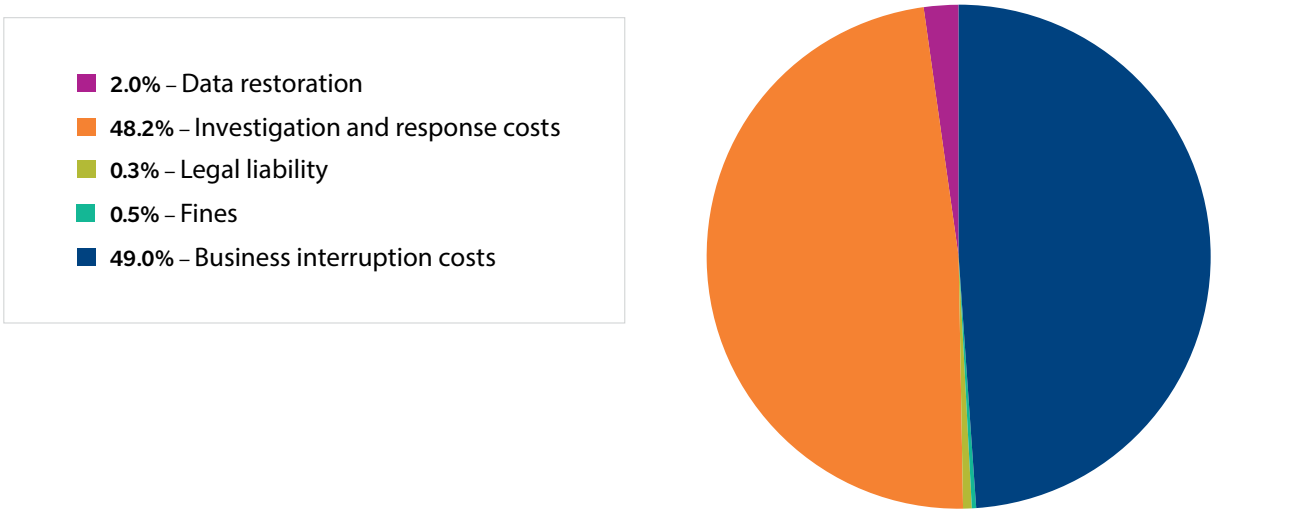
Criminals are increasingly deploying ransomware to cause maximum disruption to businesses and public institutions. For example, in March 2019, Norsk Hydro was the victim of a ransomware attack that was described by the security firm CrowdStrike as part of a trend of cyber "Big Game Hunting."

In the latest trend, criminals have leveraged more sophisticated techniques to directly deliver the ransomware payload to target networks through the use of certain combinations of vulnerabilities. This can result in the spread of ransomware to additional networks with minimal user interaction (an employee does not necessarily have to click a link in an email).

It is interesting to note that the probability of cloud service providers falling victim to a ransomware attack is much higher than the probability of a cloud outage. Cloud service providers would appear to be more vulnerable at a human level to phishing attacks, than at a systems level, to connectivity failure.

Until now, widespread ransomware and cloud outages have largely been isolated as two separate cyber scenario types for the purposes of assessing cyber-driven probable maximum

Figure 4. **Large-scale Ransomware at Leading Cloud Service Provider by Cost Component**




*Source: Guy Carpenter & CyberCube Analytics*

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 theoretical process; there was already a precedent with the July 2019 MegaCortex attack on iNSYNQ, a cloud computing provider of virtual desk environments. It is crucial for the industry to understand and avoid the dangers of too narrow a modeling perception of possible cyber events, and to be alert to how scenarios can overlap.

## Cost components

The two biggest insured loss components would be BI of USD 5.6 billion, with investigation and response costs adding USD 5.5 billion. There would also be data restoration costs of USD 234 million, fines of USD 59 million, and legal liabilities of USD 36 million.

## Considerations for insurers

The conditional loss distribution graph in this section (page 15) indicates that the volatility for this catastrophe scenario is relatively low, given it has a maximum loss at least 35 percent lower than the other scenarios discussed here. That outcome suggests this catastrophe scenario may be easier to price into individual risk assessment or to model on a portfolio of losses. The larger share of investigation and response costs highlight the value in providing post-breach services to insureds in order to help manage the cost of recovery.

"The probability of cloud service providers falling victim to a ransomware attack is much higher than that of a cloud outage."

# 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

BI costs make up the lion's share of the cost (94.4 percent). Investigation and response costs and data restoration costs make up the remainder.

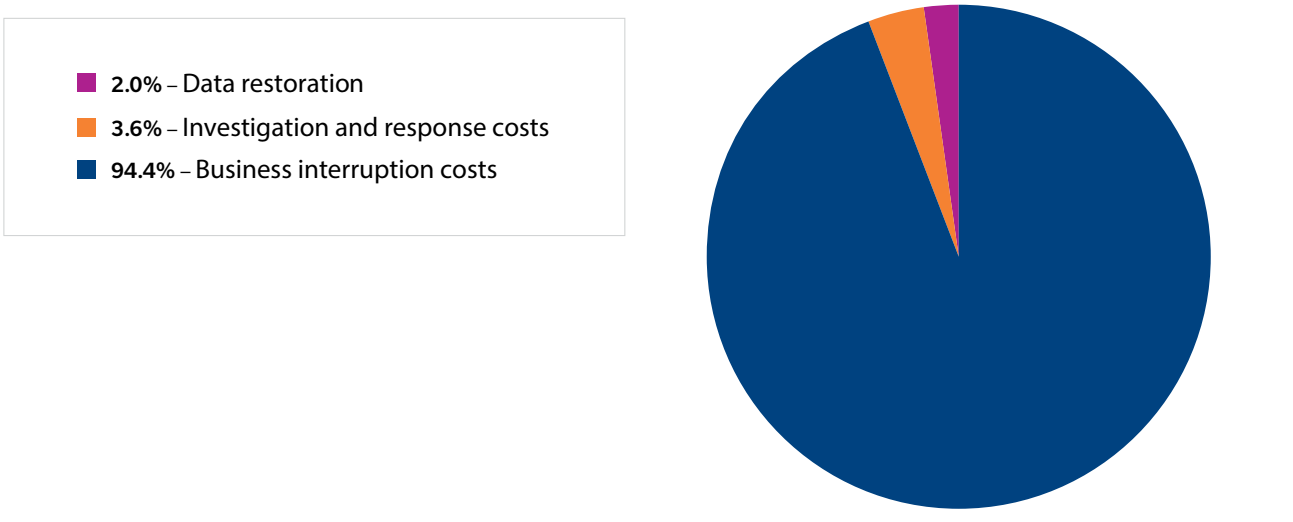
Of the 23 scenarios considered in this study, *Widespread data loss from a leading operating systems provider* and *Widespread data theft from a leading email services provider* rank in the top four for both AAL and maximum insured loss.

Table 1. **Top Four Scenarios**

| Rank | By AAL | By Maximum Insured Loss |
|---|---|---|
| 1 | Widespread Data Theft – Leading Email Services Provider | Widespread Data Loss – Leading Operating System Provider |
| 2 | Large Scale Ransomware – Leading Cloud Services Provider | Large Scale Data Loss – Leading Cloud Services Provider |
| 3 | Large Scale PoS Theft – Leading Retailer | Widespread Data Theft – Leading Email Services Provider |
| 4 | Widespread Data Loss – Leading Operating System Provider | Long Lasting Outage – Leading Cloud Services Provider |

*Source: Guy Carpenter & CyberCube Analytics*

Figure 5. **Widespread Data Loss at Leading Operating Systems Provider by Cost Component**




*Source: Guy Carpenter & CyberCube Analytics*

# **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.

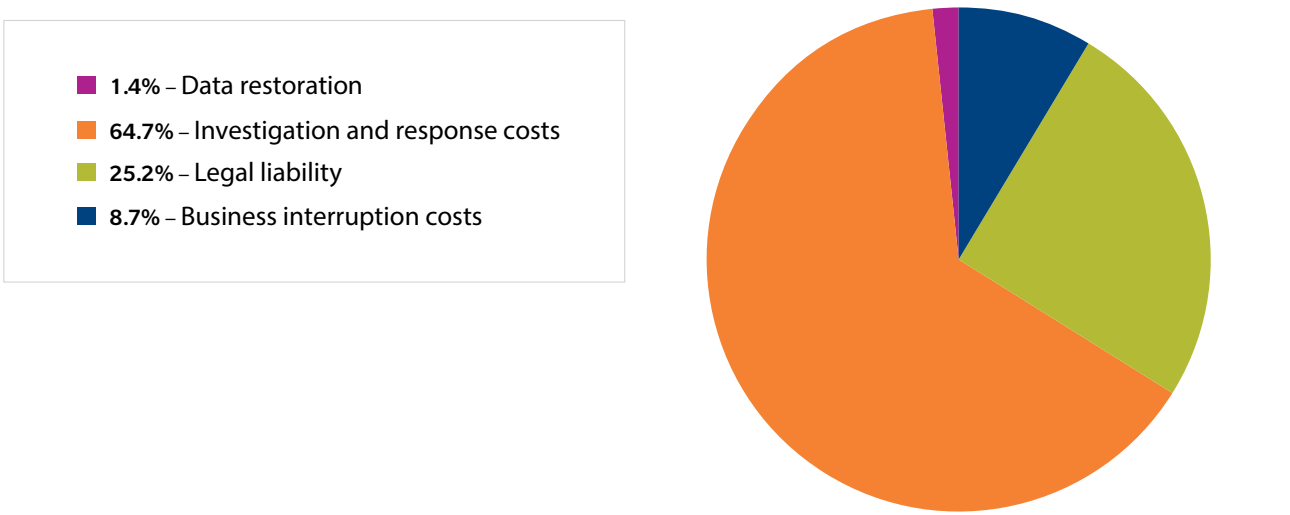
The main drivers of insured loss here are investigation costs and response costs (64.7 percent), followed by legal liability (25.2 percent). Business interruption is a minor component of this scenario, at just USD 1.7 billion (8.7 percent).

### 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. **Widespread Data Theft at Leading Email Service Provider by Cost Component**




*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.

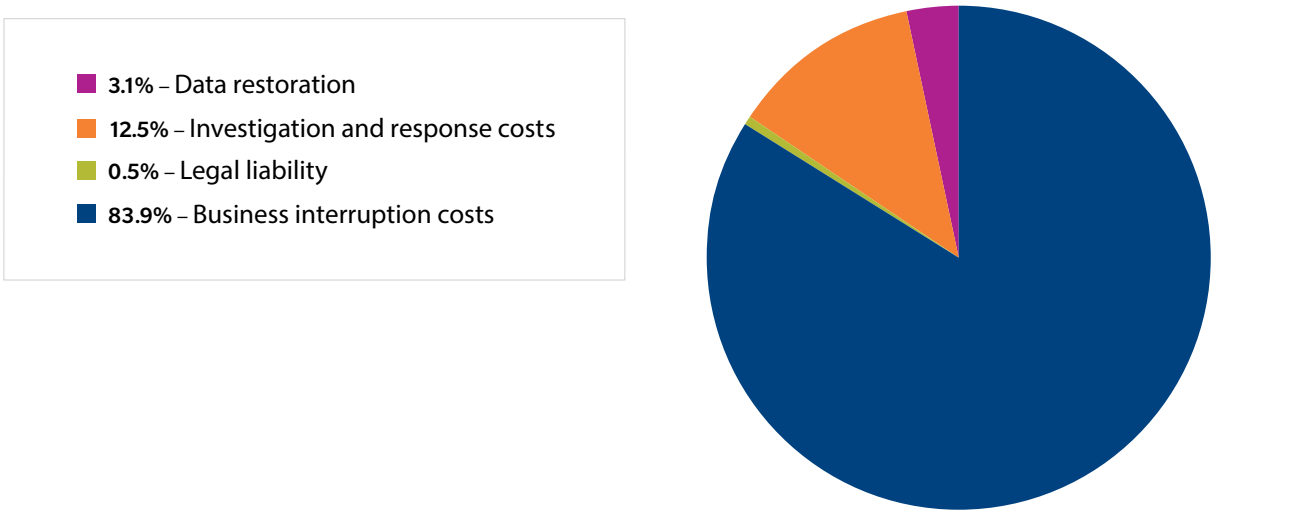
### Cost components

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.

### Considerations for insurers

The potential for BI to cause significant loss to a U.S. standalone cyber insurance portfolio is substantial. One of the drivers of this loss relates to the fact that not only does the scenario contemplate downtime at a cloud services provider, but also that the deleted data is irrecoverable. The recovery efforts by the companies impacted may involve protracted efforts to reconstitute data from varied back-up sources (where available). This is why data restoration costs increase in this scenario.

Figure 7. **Large-scale Data Loss at Leading Cloud Service Provider by Cost Component**




*Source: Guy Carpenter & CyberCube Analytics*

# 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?

Guy Carpenter and CyberCube strongly believe that taking a robust, modeled and forward-looking view of cyber catastrophe risk can help enable the cyber insurance market to grow sustainably. By combining market-leading insights with a data-driven approach, Guy Carpenter helps re(insurers) model the potential financial impacts of emerging risks and make informed risk tolerance decisions. Ultimately, sustainable growth will better position insurers to bridge the protection gap for businesses and form lasting partnerships as part of robust cybersecurity frameworks.

Future work includes expanding the scope of this analysis to include non-U.S. cyber insurance markets. We would ask for input from all stakeholders in cyber risk and insurance to collaborate with us on deepening this conversation and developing the next iteration of this study.

We hope that through this study, we have moved the conversation forward for key strategists, including CEO's, chief underwriting officers and chief risk offers; underwriters; exposure management experts; reinsurers; and catastrophe modelers.

# 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's aggregation modeling software: Portfolio Manager, to the Guy Carpenter synthetic portfolio.

Portfolio Manager includes 23 modeled systemic, catastrophic scenario classes, ranging from attacks on critical infrastructure to third-party technology aggregation scenarios to attacks that affect the cloud environment. Of these, five stood out as having the most potential to cause loss either at the mean or in an extreme event based on the synthetic U.S. portfolio.

The CyberCube Enterprise Information Layer is a terabyte-scale database that draws on a diverse range of sources, each providing an important perspective on cyber risk. It is curated into four categories:

- **Enterprise data** provides crucial information on the operations and exposure of millions of companies, ranging from micro to large and global.
- **Internal security data** generates insights through exclusive "behind-the-firewall" data not available to (re)insurers. It enables superior assessment of vulnerabilities and threats operating inside networks.
- **External security data** is derived from the specific observation of threats and vulnerabilities from outside protected networks.
- Claims data provides parameters that inform the calibration of results.

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 of accumulations of exposure within a portfolio of insured companies.

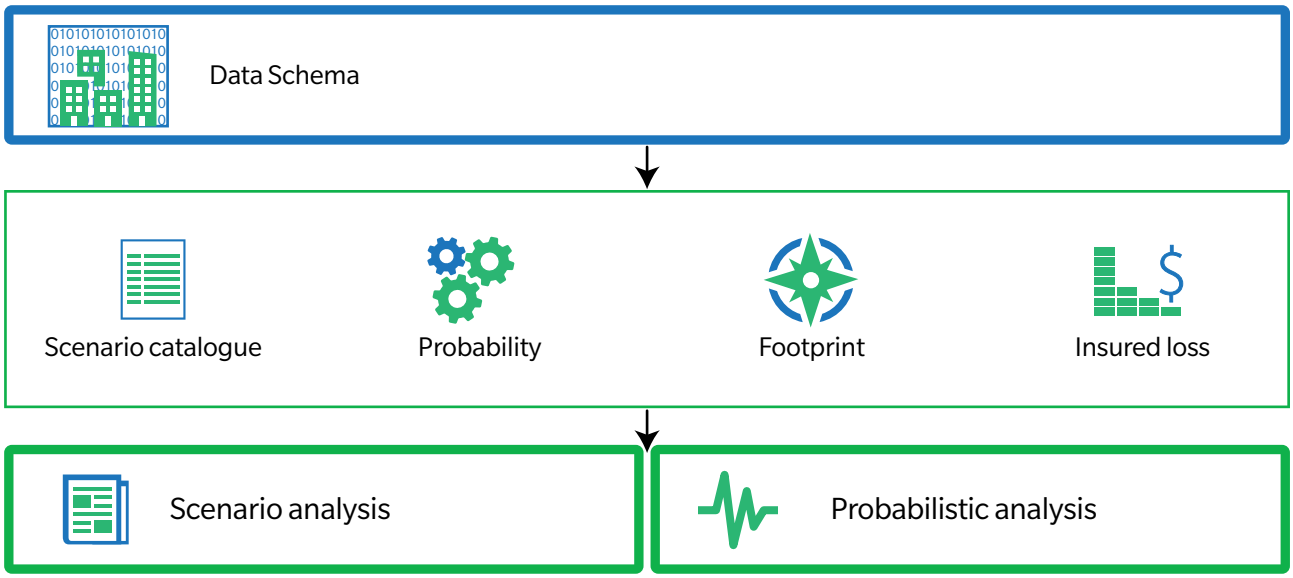
**Insured loss** is calculated for a range of specific coverages, enabling the drivers of loss to be identified and analyzed. Losses are calculated "ground up" and then applied to the specific limits and deductibles included in the portfolio. This generates an accurate picture of actual (re)insured exposure, as opposed to broad economic exposure.

This powerful engine drives two complementary forms of output: scenario analysis, which applies the insights of our Enterprise Intelligence Layer to specific conditions; and probabilistic analysis, which measures the entire set of scenario classes at varying return periods.

**Scenario analysis** is widely used in the cyber (re)insurance market, usually against events that are defined in qualitative terms such as "realistic disaster" or "plausible but extreme." Portfolio Manager enhances this approach with the application of event probabilities, enabling cyber risk to be managed with insight comparable to other catastrophe exposures.

**Probabilistic analysis** elevates the art of cyber risk estimation to the science of catastrophe risk management. The scale and depth of the CyberCube Enterprise Intelligence Layer unlocks the power of well-established techniques applied in other data-rich classes of (re)insurance, such as stochastic event simulation and year loss tables, to inform capital allocation, exposure management and catastrophe risk loading.

## High-level architecture and outputs of Portfolio Manager



## 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 percent of the U.S. cyber market. To extrapolate to a 100 percent U.S. market view, an additional 49,000 additional policies were added to create a new total premium of USD 2.6 billion, known as the modeled portfolio.

The modeled portfolio consists of U.S. risks only and are standalone, affirmative cyber policies. Excluded from the portfolio are endorsements, package policies and non-affirmative cyber potentially included in other lines of business. The portfolio preserved original policy terms, including: revenue, company size, industry, limit, attachment, sub-limits and premiums.

All of the modeled results are based on 10,000 simulations using the CyberCube platform. To expand subject premium from USD 285 million to an industry-sized level (USD 2.6 billion in the United States), Guy Carpenter utilized a few extension approaches. Specifically, Guy Carpenter developed notional industry-size portfolios representing a range of extension continuum possibilities:

1. Extend by adding Micro-only risks
2. Extend by adding Large-only risks
3. Extend using proportion of risk sizes seen in underlying exposure dataset.

Ultimately, the option to extend the portfolio using the proportion of risk sizes in the underlying portfolio was selected to provide a view most representative of actual written policies.

To analyze catastrophic risk potential across a wide spectrum of attack types, Guy Carpenter conducted extensive stress testing using CyberCube's probabilistic model within Portfolio Manager v1.6. This probabilistic analysis simultaneously considers all scenarios from the extensive CyberCube scenario catalog and allows for any relevant SPOF to be affected. There are numerous settings available when running an analysis to allow various stress tests and to isolate various components of the modeled loss for granular insights. These settings include frequency levels of Low, Default and High; frequency distributions of Poisson or Negative Binomial; and sub-limits for various cost components within the model. The frequency settings are a valuable mechanism to test one of the most common differing views of risk discussed in this report: the likelihood of these catastrophes occurring.

The Low frequency view can be applied for the view of less active or less sophisticated threat actors and/or better defended targets. This also can apply for portfolios where strong risk selection controls are in place and the pre- and post-breach service offered would provide meaningful loss mitigation and controls. The high-frequency mode can be used for analyses meant to examine a portfolio under extreme stress. The greatly increased frequency of events due to very active and sophisticated threat actors can provide an upper bound to the potential loss of a portfolio.

CyberCube's Portfolio Manager was used to run 60 iterations of the base portfolio to identify a range of outputs, including:

- BI included or excluded
- The BI waiting time
- Whether the frequency of event was low, default or high
- Whether the frequency distributional family was Poisson (giving the probability of a number of independent events occurring in a fixed time) or Negative Binomial (the probability of a number of independent event successes before a fixed number of failures).

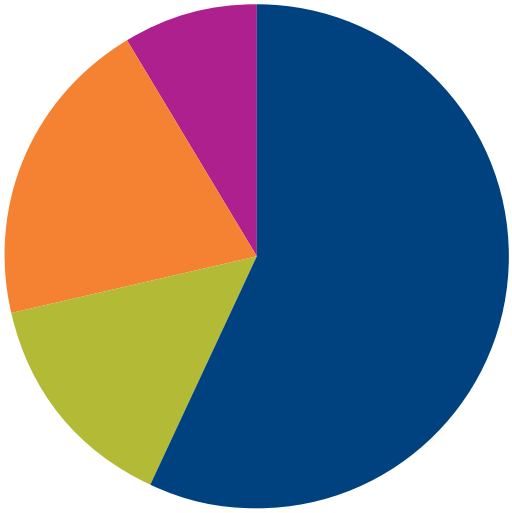
Ultimately, the risks were modeled using the following settings, which most closely reflect industry standard:

- Default frequency
- Poisson distribution
- No insured name
- Actual BI waiting periods where explicitly available, assumed to be eight hour waiting period when not provided.

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

## Figure 8. Portfolio Premium by Size of Business

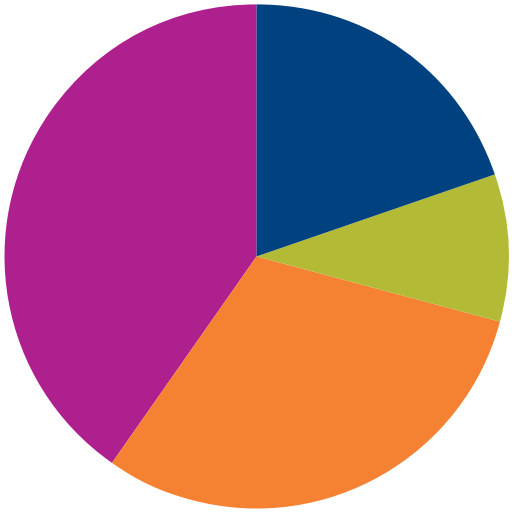
- **8.6%** – Micro (<$10mn revenue)
- **19.9%** – Small ($10mn-$250mn revenue)
- **14.5%** – Medium ($250mn-$1bn revenue)
- **57%** – Large (>$1bn revenue)



*Source: Guy Carpenter & CyberCube Analytics*

## Figure 9. Portfolio Policy Count by Size of Business

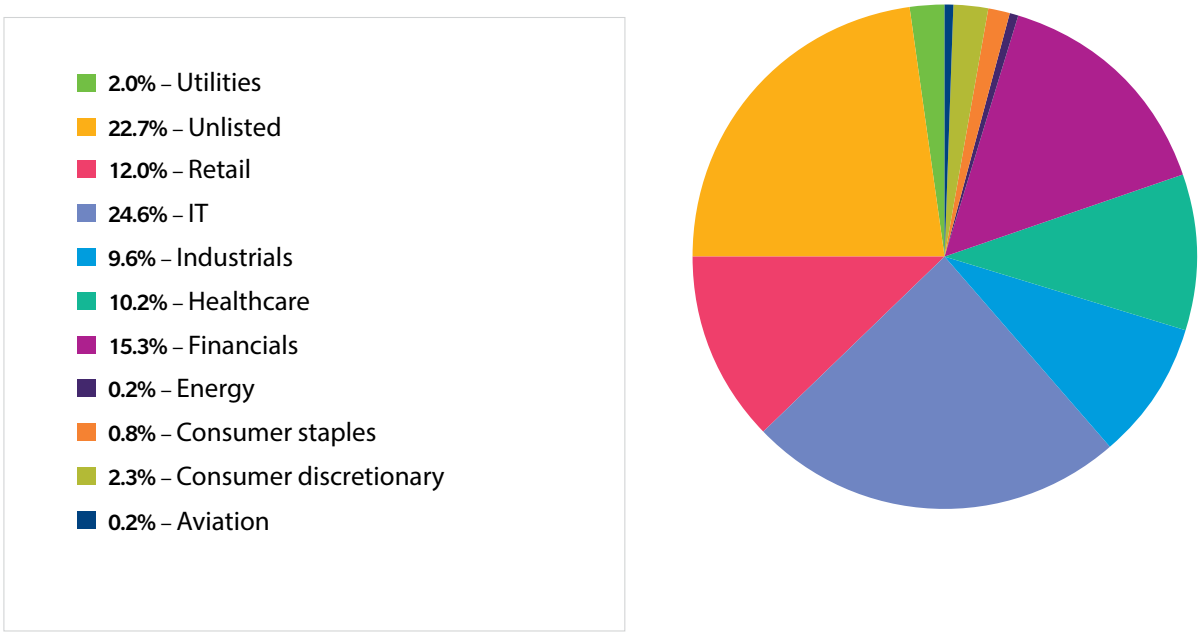
- **40.1%** – Micro (<$10mn revenue)
- **30.8%** – Small ($10mn-$250mn revenue)
- **9.4%** – Medium ($250mn-$1bn revenue)
- **19.8%** – Large (>$1bn revenue)



*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.

Figure 10. **Portfolio Premium Breakdown by Industry**




**To learn more about how our solutions bring profitable growth to your businesses, please contact:**

**Siobhan O'Brien,** *Cyber Center of Excellence, Guy Carpenter:* Siobhan.Obrien@guycarp.com

**Jeremy S. Platt,** *Cyber Center of Excellence, Guy Carpenter:* Jeremy.S.Platt@guycarp.com

**Erica Davis,** *Cyber Center of Excellence, Guy Carpenter:* Erica.Davis@guycarp.com

**Christopher Shafer,** *Cyber Center of Excellence, Guy Carpenter:* Christopher.Shafer@guycarp.com

**Rebecca Bole,** *Head of Industry Engagement, CyberCube Analytics:* Rebeccab@cybcube.com

**Yvette Essen,** *Head of Content and Communications, CyberCube Analytics:* Yvettee@cybcube.com

We acknowledge contributions from Joshua Pyle (Actuarial Director) and Emma Ye (Senior Predictive modeler), CyberCube Analytics.

GUY CARPENTER

**About Guy Carpenter**

Guy Carpenter & Company, LLC is a global leader in providing risk and reinsurance intermediary services. With over 60 offices worldwide, Guy Carpenter creates and executes reinsurance solutions and delivers capital market solutions* for clients across the globe. The firm's full breadth of services includes line-of-business expertise in agriculture; aviation; casualty clash; construction and engineering; excess and umbrella; life, accident and health; marine and energy; medical professional liability; political risk and trade credit; professional liability; property; retrocessional reinsurance; surety; terrorism and workers compensation. GC Fac® is Guy Carpenter's dedicated global facultative reinsurance unit that provides placement strategies, timely market access and centralized management of facultative reinsurance solutions. In addition, GC Analytics® utilizes industry-leading quantitative skills and modeling tools that optimize the reinsurance decision-making process and help make the firm's clients more successful. For more information, visit www.guycarp.com. Guy Carpenter is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With nearly 76,000 colleagues and annual revenue over $17 billion, through its market-leading companies including Marsh, Mercer and Oliver Wyman, Marsh & McLennan helps clients navigate an increasingly dynamic and complex environment. For more information, visit www.guycarp.com. Follow Guy Carpenter on Twitter @GuyCarpenter.

*Securities or investments, as applicable, are offered in the United States through GC Securities, a division of MMC Securities Corp., a US registered broker-dealer and member FINRA/SIPC. Main Office: 1166 Avenue of the Americas, New York, NY 10036. Phone: (212) 345-5000. Securities or investments, as applicable, are offered in the European Union by GC Securities, a division of MMC Securities (Europe) Ltd., which is authorized and regulated by the Financial Services Authority. Reinsurance products are placed through qualified affiliates of Guy Carpenter & Company, LLC. MMC Securities Corp., MMC Securities (Europe) Ltd. and Guy Carpenter & Company, LLC are affiliates owned by Marsh & McLennan Companies. This communication is not intended as an offer to sell or a solicitation of any offer to buy any security, financial instrument, reinsurance or insurance product.

**About CyberCube**

CyberCube delivers the world's leading cyber risk analytics for the insurance industry. With best-in-class data access and advanced multidisciplinary analytics, the company's Software as a Service platform helps insurance companies make better decisions when underwriting cyber risk and managing cyber risk aggregation. CyberCube's enterprise intelligence layer provides insights on millions of companies globally and includes modeling on over one thousand single points of technology failure. The CyberCube platform was established in 2015 within Symantec, the global leader in cybersecurity, and now operates as a standalone company exclusively focused on the insurance industry, with continued access to Symantec data and resources and backing from ForgePoint Capital. For more information, please visit www.cybcube.com or email info@cybcube.com

**Disclaimer**

Guy Carpenter & Company, LLC provides this report for general information only. The information contained herein is based on sources we believe reliable, but we do not guarantee its accuracy, and it should be understood to be general insurance/reinsurance information only. Guy Carpenter & Company, LLC makes no representations or warranties, express or implied. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such. Please consult your insurance/reinsurance advisors with respect to individual coverage issues.

Statements concerning tax, accounting, legal or regulatory matters should be understood to be general observations based solely on our experience as reinsurance brokers and risk consultants, and may not be relied upon as tax, accounting, legal or regulatory advice, which we are not authorized to provide. All such matters should be reviewed with your own qualified advisors in these areas.

Readers are cautioned not to place undue reliance on any historical, current or forward-looking statements. Guy Carpenter & Company, LLC undertakes no obligation to update or revise publicly any historical, current or forward-looking statements, whether as a result of new information, research, future events or otherwise.



MARSH & McLENNAN COMPANIES