GuyCarpenter

UNDER THE LENS:

Investigating Cyber Vendor Model Divergence

A business of Marsh McLennan

REPORT HIGHLIGHTS

- While significant progress has been made in advancing cyber catastrophe vendor models over the past decade, a notable degree of variability across model outputs still exists. Having clarity in the drivers of this model variability helps cyber carriers establish their unique views of risk, which in turn supports exposure management and capacity deployment decisions.
- Annual revenue input results in the highest modeled loss differences, with the greatest model divergence concentrated in the nano (<USD 1 million) and micro (USD 1 million to USD 5 million) revenue bands. This warrants a deeper understanding of different models' treatments of low-revenue organizations, as the cyber market continues its expansion in the small and micro risk segments.
- Industry sector classification is the second most impactful driver of model variability. The retail sector in particular leads to substantial divergence across vendor models, as a result of differences in vendors' view of top loss contributors.
- Vendor models' differing treatment of specific coverages, such as Ransomware & Extortion and Regulatory Defense & Fines, highlights the challenges with aligning diverse cyber policy wordings with available model functionality.

CONTENTS

INTRODUCTION & METHODS

Among the greatest challenges for cyber writers is constructing their own view of risk to manage cyber exposure accumulation in order to support decisions around capacity constraints and capital deployment. Over the past decade, tremendous progress has been made in the area of cyber risk quantification, including development of a multitude of cyber catastrophe models using a wide range of differing techniques and methodologies.

The models' results are gradually converging over time as more credible data points become available for calibration and validation. However, a notable degree of variability across model outputs still exists, which can pose a challenge to insurance and reinsurance companies as they formulate a unique view of risk. Guy Carpenter began exploring this subject at the industry level in our recent report, *Through the Looking Glass: Interrogating the Key Numbers Behind Today's Cyber Market*.[1] In this study, a companion to the earlier report, our team conducts an in-depth investigation into the key drivers of cyber catastrophe model differences. This study aims to provide a level of comfort to cyber market participants in constructing their own views of exposure accumulation as their books expand and evolve.

1. What is the question?

As cyber catastrophe models are being relied upon increasingly by insurers and reinsurers to make strategic decisions, it is crucial to establish a more informed view of the driver behind these models' variability. In this study, we applied advanced analytics using predictive modeling to achieve a deeper and more robust understanding of key factors driving divergence in cyber model outputs.

2. Why predictive analytics?

The current industry approach for evaluating cyber model output relies heavily on the availability of individual vendor model insights and expert judgment around the appropriateness of underlying model methodology. This approach lacks objective model analysis and can be subject to bias from subjective opinion. Advanced analytics today can support a new approach in assessing differences across modeled output. Utilizing the latest sophisticated predictive-modeling tools synthesizes the complete array of input parameters flowing into the cyber model, including company characteristics and policy structure, as well as numerous elected coverages.

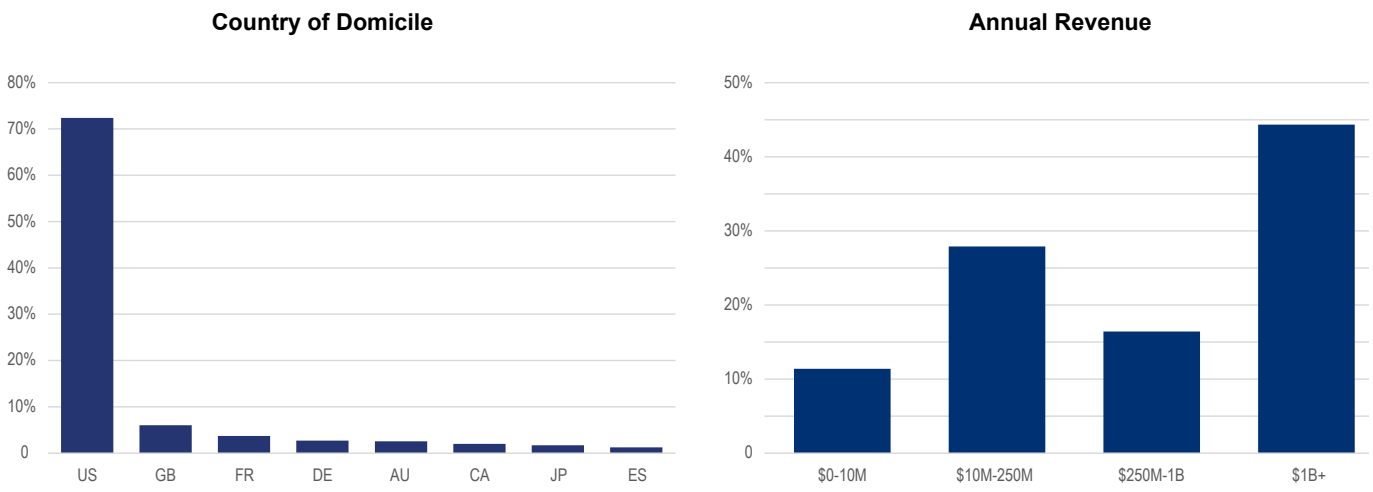
3. How did we start?

We focused our effort to understand the differences between 3 major cyber models—Guidewire Cyence, CyberCube, and Moody's RMS. There were 3 key points we aimed to address:

- Which input parameters drive the greatest cyber model divergence?
- Identify market segments where industry view of risk is most divergent.
- Highlight risk characteristics for which a given cyber model may yield a significant average annual loss (AAL) penalty.

To address these points, we relied on a sampled company-level dataset that approximated the distribution of the cyber industry, including key input parameters that Guy Carpenter compiles across available vendor models. The following figures illustrate the sample dataset's premium distribution by annual revenue and country of domicile.

Figure 1: Premium distribution by annual revenue and country of domicile



Source: Guy Carpenter proprietary information from Guy Carpenter Cyber Data Lake.

1. https://www.guycarp.com/content/dam/guycarp-rebrand/pdf/Insights/2023/Guy_Carpenter_Cyber_(Re)insurance_Market_Report_Publish_rev%20.pdf

The dataset was then modeled using each of the 3 cyber models to generate an AAL at the individual-company level, as well as a portfolio average.

4. Our technical approach

To properly analyze the drivers of model variability, it is important to control for the effect of all available input parameters. Relying on a simple one-way analysis may show model divergence across different geographies, but would fail to account for varying risk distributions within each geography, for example, US may include business with higher annual revenues when compared with other countries. Leveraging the latest non-linear machine learning techniques allows us to control for the effect of all other variables and best isolate the signal from the noise. However, any application of machine learning should be paired with the necessary subject-matter expertise for the best possible outcome. Our unique ability to incorporate sophisticated modeling algorithms with leading cyber expertise offers the most detailed understanding of cyber catastrophe models to date.

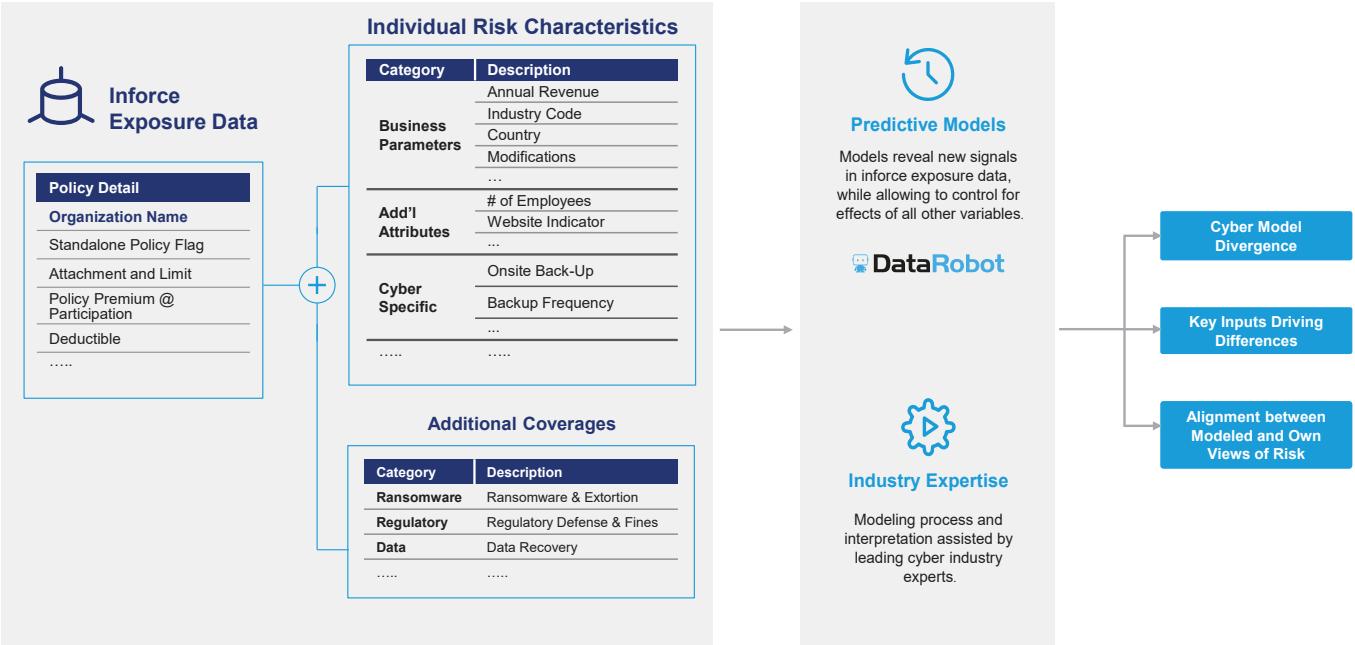
We elected to model the coefficient of variation across each policy using individual cyber input parameters as predictors to answer where cyber models yield the most disagreement of ultimate potential for catastrophe event loss.

THERE IS NO SINGLE DRIVER OF CYBER MODEL DIVERGENCE IN OUR STUDY, RATHER A VARYING COMBINATION OF MULTIPLE PARAMETERS THAT DRIVES THE DISCREPANCY IN MODELED AALS.

Figure 3 shows a ranking of variables according to their relative impact on cross-model variability. As an example, company annual revenue is the most divisive input parameter, resulting in the greatest disagreement in perceived risk across the 3 cyber models. On the other hand, there appears to be little disagreement in perceived risk from a number of company employees, after accounting for all other input parameters.

One interesting takeaway from this chart is the distribution of individual risk characteristics, policy

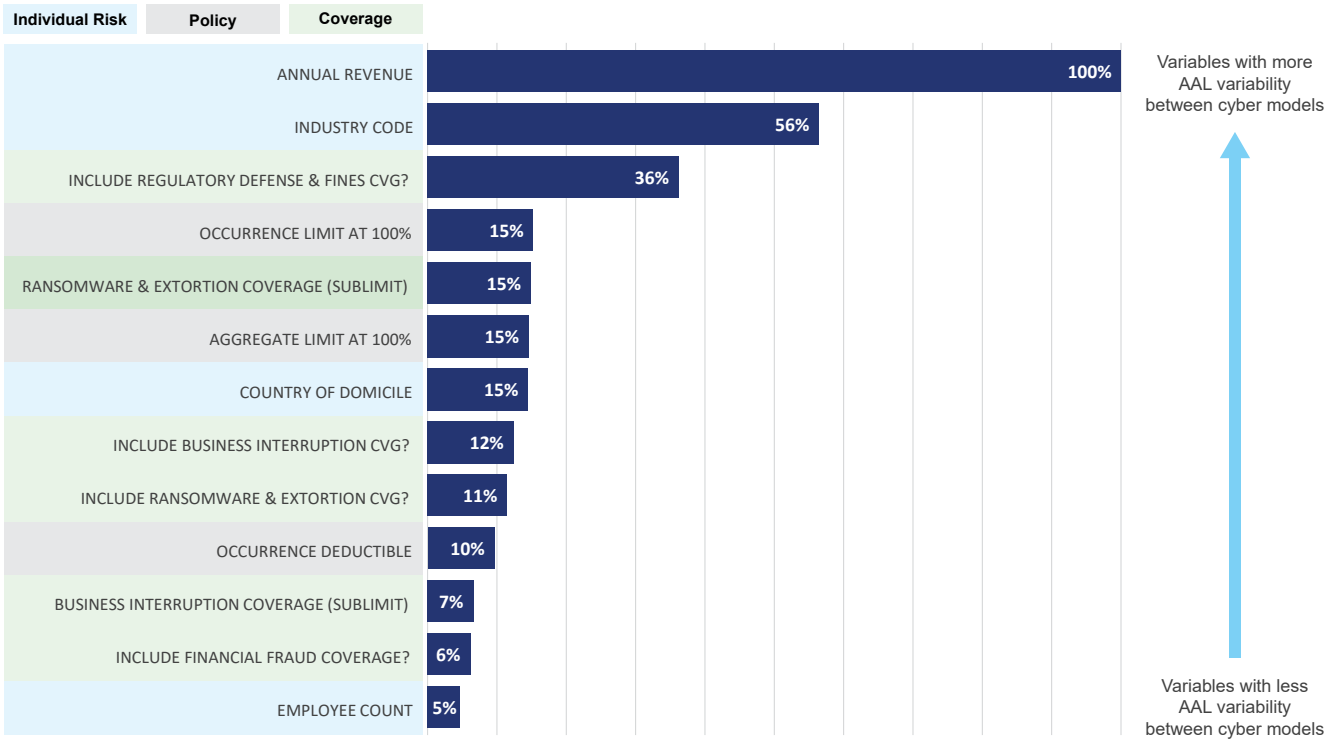
Figure 2: Guy Carpenter Predictive Modeling Process—Understanding Differences Across Major Cyber Models



attributes and coverage elections. Specifically, there is no single driver of cyber model divergence in our study, rather a varying combination of multiple parameters that drives the discrepancy in modeled AALs.

After obtaining a fundamental baseline view of model divergence, we focused on the unique biases found within each cyber model. In other words, which level of annual revenue or specific industry codes results in the highest AAL in a particular cyber model. This was accomplished by focusing on the AAL ratio between any 2 given models to highlight portfolio segments with greatest spread.

Figure 3: Relative Importance to Model Variability



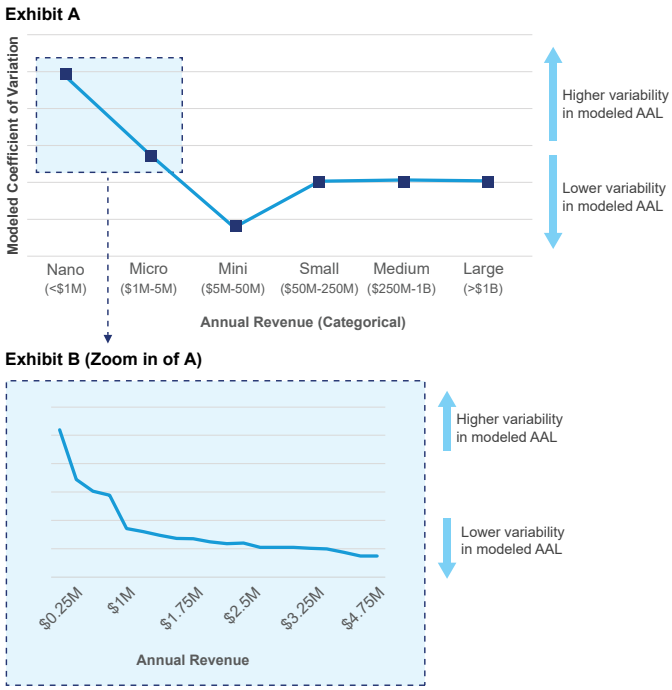
Note: All importance metrics are relative to the variable with the highest importance.

Source: Guy Carpenter study based on outputs from Guidewire Cyence, Moody's RMS, and CyberCube.

KEY OBSERVATIONS

As discussed in *Through the Looking Glass: Interrogating the Key Numbers Behind Today's Cyber Market*, Guy Carpenter always recommends focusing as much on the "why" as the "how much" of model divergence. Using the robust framework of predictive modeling, Guy Carpenter is able to highlight some of the key data items that drive loss variability across vendor models.

Figure 4: Model Variability—Annual Revenue



Source: Guy Carpenter study based on outputs from Guidewire Cyence, Moody's RMS, and CyberCube.

Revenue

The clear driver of loss variability across the 3 tested vendor models is revenue. Revenue is inherently connected to key cyber loss types, such as business interruption (BI), contingent business interruption (CBI) and data restoration. As such, it is expected that modeled losses will increase as revenue increases. However, variability in modeled results decreases as revenue increases.

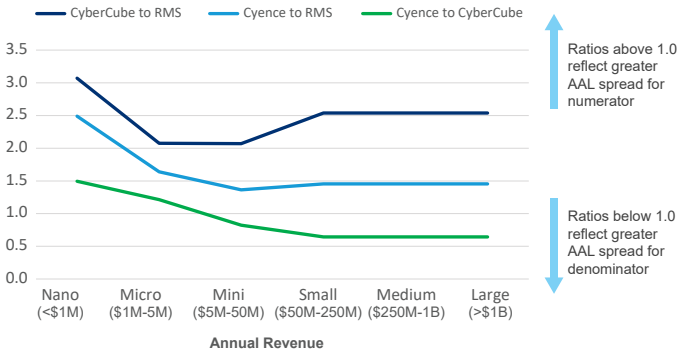
This is very much in line with our understanding of the data environment, in which the models were constructed as a direct consequence of the availability of data for different revenue ranges. Incident, firmographic and technographic data are quite readily available for large entities, such as those in the Fortune 500 index, but are considerably reduced as we approach micro and mini risks. There is much more room for differing treatments of available data, as well as expert judgment to fill out the missing areas of data at the lowest level of company revenue size.

The cyber insurance market continues to see increased penetration in the small revenue space, which will increase attention on the reliability of modeling for very small risks. As granular data collection becomes a higher priority in the cyber industry, we should expect to see a decrease in the variability of results in this space. Beyond the USD 5 million range, we found that the variability of results was very consistent out to truly large risks, with revenue greater than USD 1 billion.

The variability seen in the smallest revenue bands will be worth extra attention due to the increasing volume of policies written in that area. A deeper understanding of the relative treatments of low-revenue organizations by the vendor models will be essential to the alignment of internal views of risk to vendor views.

In our analysis, CyberCube and Guidewire Cyence were both more conservative than Moody's RMS across all revenue bands in their estimates of loss for micro and mini risks. Guidewire Cyence exhibits a more conservative view than CyberCube for these risks but produces relatively lower results for higher revenue bands. Moody's RMS showed the least differentiation in results across revenue bands.

Figure 5: Modeled AAL Relativity by Revenue Size

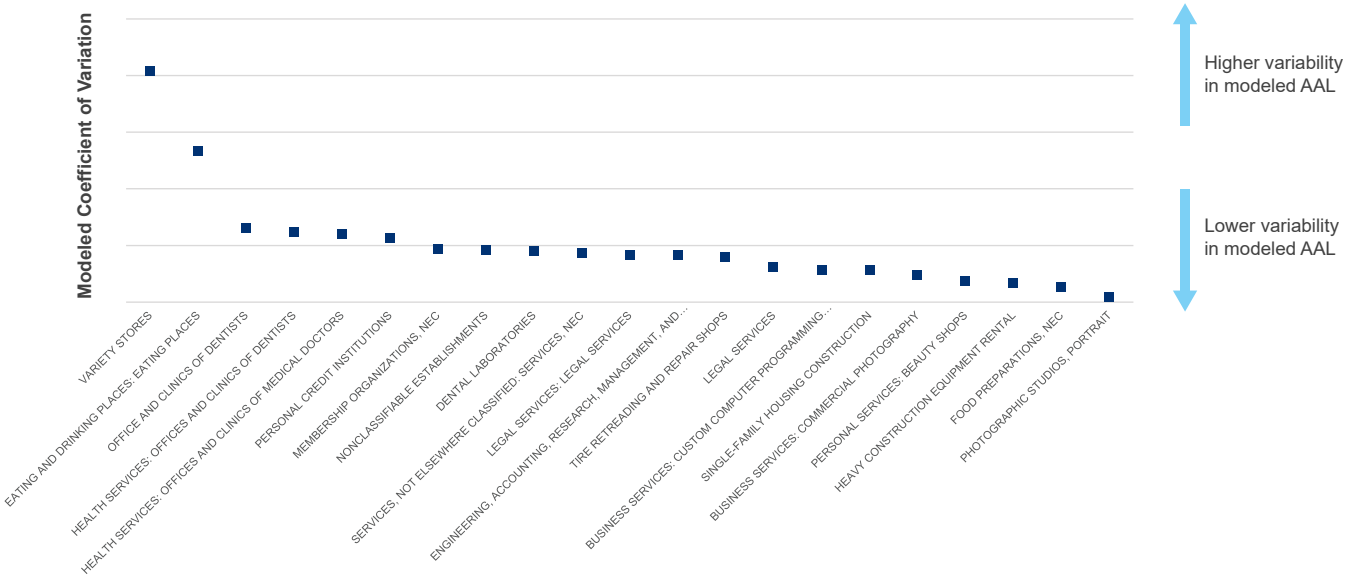


Source: Guy Carpenter study based on outputs from Guidewire Cyence, Moody's RMS, and CyberCube.

Industry

The results of the study indicate that industry sector is the second-most-impactful driver of variability in losses. Industry sectors differ in how they carry out their business. This necessarily means that technologies utilized across sectors also will vary and will be relied upon to different extents. Different sectors may also vary in their security posture, resiliency and attractiveness to threat actors. As a result, conceptually, industry sector will have a significant impact on cyber

Figure 6: Model Variablility—Industry Sector



Source: Guy Carpenter study based on outputs from Guidewire Cyence, Moody's RMS, and CyberCube.

loss. We also find that this area causes significant variability in losses across vendor models.

Each vendor model has made a conscious and independent decision on the level of granularity for parameterizing their model framework, especially along the dimension of industry sector classification. There are various code schemes and significant numbers of underlying codes at differing granularities that can be used to represent the differences between industry sectors. It is unsurprising that the different classification approach taken by each vendor model leads to additional model variability.

All 3 models parameterize based on internal codes schemes. CyberCube's 21 sectors and Guidewire Cyence's 18 sectors are simplified views of Standard Industrial Classification (SIC) codes, while Moody's RMS uses a 34-code simplification of North American Industry Classification System (NAICS) codes. SIC and NAICS code schemes were created at different times and have varying granularities for some sectors. In particular, the NAICS system was created because of a desire for a code scheme that better represented current industry sectors. In some cases there are many-to-one or one-to-many translations between the 2 code schemes. Additionally, the differing number of codes in the vendor model industry schemes helps to illustrate the divergence in vendor model views around industry sectors. The parameterization of each of these segments will be directly impacted by the source data that is aggregated into them, driving the variability we see in our investigation.

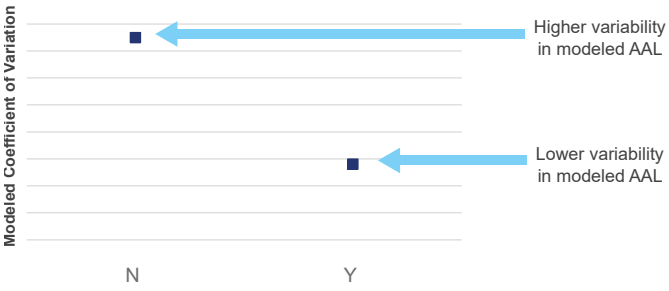
The study shows that, by a significant margin, the Variety Stores and Eating and Drinking Places sectors are the main drivers of variability in vendor model results. Both of these sectors map to the retail sector in all 3 models. Investigation found that this variability is driven in large part by CyberCube's more conservative view of the retail industry sector. As noted in *Through the Looking Glass: Interrogating the Key Numbers Behind Today's Cyber Market*, CyberCube's scenario parameterization considers financial fraud to be a significant contributor to loss, and this is tied closely with payment processor events that heavily impact the retail sector.

Through the Looking Glass: Interrogating the Key Numbers Behind Today's Cyber Market notes that ransomware and malware events are top event drivers for modeled losses across vendors as well as being broadly agreed upon as a major driver of loss across the industry. Notwithstanding this observed commonality in modeled result, our study identifies that there are differing interpretations and treatments to the Ransomware & Extortion Coverage indicator across the models.

In Figure 7 on the next page, there is an obvious impact on model variability when Ransomware & Extortion Coverage is included. Each vendor model allows for varied options for importing coverage and sublimit information. Moody's RMS allows for the widest range of coverages, with 16 distinct options, including a specific cyber extortion coverage. CyberCube offers 7 coverage options, but as of Version 4, Portfolio Manager (PM) does not have functionality for ransomware-specific coverage inclusion. Ransomware payments are currently reflected in CyberCube as a part of the Investigation & Response

cost component. It is valuable to note that CyberCube's release of PMv5 will include Ransom & Extortion as a distinct cost component. Guidewire Cyence offers 5 distinct coverages, which include a cyber extortion option. The results from CyberCube, where ransomware costs are embedded in the Investigation & Response Coverage, are the driving element for divergence under this coverage. Unlike in property, where policy wordings are far more homogeneous, cyber policies are written with differing coverages using diverse definitions for each. Until the space becomes more standardized, there will continue to be challenges in aligning policy wordings with available model functionality.

Figure 7: Model Variability—Ransomware & Extortion Coverage

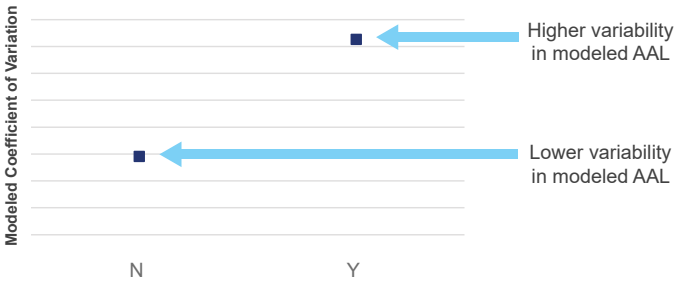


Source: Guy Carpenter study based on outputs from Guidewire Cyence, Moody's RMS, and CyberCube.

Regulatory Defense & Fines

The Regulatory Defense & Fines coverage, like Ransomware & Extortion, is indicative of the varying views on coverage options by the vendor models but also illustrates the differing approaches taken in defining cyber scenarios. In this case, Moody's RMS and CyberCube have explicit coverages for Regulatory Defense & Fines, with Guidewire Cyence not explicitly allowing for coverage inclusion or exclusion. The difference in options, however, results in a similar picture. Including Regulatory Defense & Fines coverage will increase divergence in the models. More specifically, CyberCube AAL will increase as a ratio to Guidewire Cyence with the inclusion of the Regulatory Fines & Defense Coverage. It is also interesting to note that Guidewire Cyence and Moody's RMS take a more general view on the types of fines considered in their scenarios, broadly including Personal Health Information (PHI), Personally Identifiable Information (PII), and Payment Card Industry (PCI) fines. CyberCube, on the other hand, is much more prescriptive in their view of fines, by making explicit inclusions of fines based on the detailed narratives used in their scenario catalogue.

Figure 8: Model Variability—Regulatory Defense & Fines Coverage



Source: Guy Carpenter study based on outputs from Guidewire Cyence, Moody's RMS, and CyberCube.

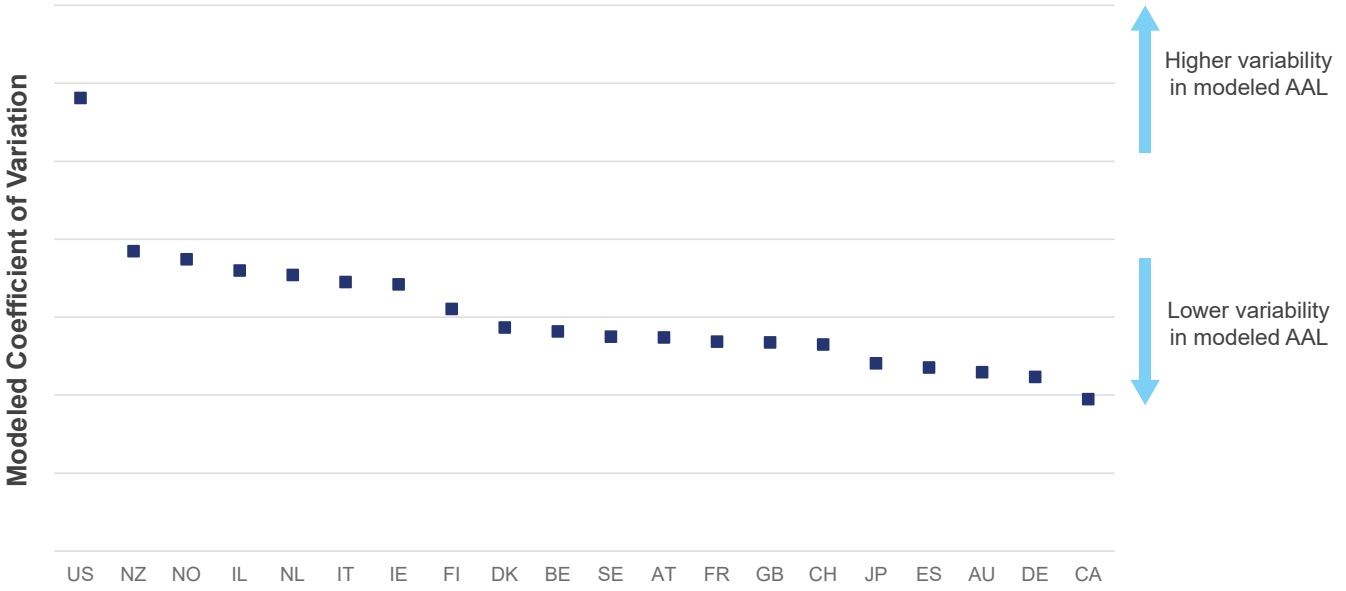
Country of Domicile

Through the Looking Glass: Interrogating the Key Numbers Behind Today's Cyber Market discusses the impacts of differing regional views of vendor models. While not a top driver of variability, this study notes that some model variation is driven by country of domicile. This provides an opportunity to explore the vendor model approaches to regional differences.

Each vendor has parameterized their models differently with regard to geography, especially within the scope of cloud outage events. For their cloud outage model, Moody's RMS views the world in 3 cloud regions: US, Europe, and Asia Pacific. CyberCube's footprint factors are defined by 5 regions: Americas, Europe, Asia, Africa, and Oceania. CyberCube's severity factors, however, are defined as US, UK, Germany, France, Japan and all others. It is also valuable to note that of the 8 cloud-related CyberCube scenarios, 7 are of global scope, with the remaining one focused on US only. Guidewire Cyence's service provider scenario, which includes cloud outage, has the highest granularity and is parameterized at the state or province granularity for US and Canada and by country for all other areas. The differentiation in geographic definitions and scopes, especially for the US, which is grouped or divided differently in each model, will clearly cause some variability in the models.

CYBER POLICIES ARE WRITTEN WITH DIFFERING COVERAGES USING DIVERSE DEFINITIONS FOR EACH. UNTIL THE SPACE BECOMES MORE STANDARDIZED, THERE WILL CONTINUE TO BE CHALLENGES IN ALIGNING POLICY WORDINGS.

Figure 8: Model Variability—Country of Domicile



County codes: *US (United States); NZ (New Zealand); NO (Norway); IL (Israel); Italy (IT); (IE) Ireland; FI (Finland); DK (Denmark); BE (Belgium); SE (Sweden); AT (Austria); FR (France); GB (Great Britain); CH (Switzerland); JP (Japan); ES (Spain); AU (Australia); DE (Germany); CA (Canada)*

Source: Guy Carpenter study based on outputs from Guidewire Cyence, Moody's RMS, and CyberCube.

CONCLUSIONS & LOOK AHEAD

As the global cyber market is quickly reaching a critical mass with no sign of slowing down, it is becoming a much more significant constituent of the insurance industry. Cyber catastrophe modeling capabilities are evolving alongside the market in their methodology and approaches. The robustness of the various modeling platforms has reached a point of maturity where predictive analytics can be applied to investigate the drivers of model divergence and variability.

This Guy Carpenter study is made possible by the unique blend of credible proprietary data with rich company-level details, deep expertise in cyber risk and catastrophe modeling, and powerful predictive analytics capabilities. Armed with the insights generated by this study, cyber industry participants can achieve better visibility into the relative importance of inputs driving model results, enabling them to construct a view of risk that most appropriately balances portfolio characteristics and model nuances.

Our report provides the data-driven support behind the general market perception that revenue is a key driver of model differences. However, many other exposure dimensions, such as industry subclass and treatment of specific coverages, also affect various models in different ways. Attaining a full understanding of divergence in results requires combining an appreciation of the models' nuances with subject-matter expertise to opine on output reasonability. This study contextualizes the technical observations from predictive analytics with real-world cyber-catastrophe considerations.

Model vendors update their models regularly in order to offer greater functionality and to keep up with a rapidly changing marketplace.

With each new update, cyber models are becoming ever more sophisticated and robust. To give credit for the progress of each model vendor, continuous assessment of the results and variability included in this study are required to keep up with the model's evolution. Using firmographic data and looking at results on an expected-loss level is the first step in the effort to understand and quantify model divergence. We will update this study as new model versions are released. Additionally, we will incorporate enhancements, such as interrogation of the relationship between real-world company-level technographic information/security posture and model divergence at tail return periods.

BY MARRYING CYBER CATASTROPHE MODELING EXPERTISE AND PREDICTIVE ANALYTICS, THIS STUDY HELPS INSURERS AND REINSURERS IDENTIFY MARKET SEGMENTS WHERE THE MODEL VIEW OF RISK IS MOST DIVERGENT.

Insurance and reinsurance companies are constructing their own views of risk based on vendor cyber aggregation models in order to manage cyber exposure accumulation. By marrying cyber catastrophe modeling expertise and predictive analytics, this study helps insurers and reinsurers identify market segments where the model view of risk is most divergent. This will result in more confidence for insurers and reinsurers in making decisions about their deployment of capacity, which ultimately supports the cyber industry's sustainable growth forward.

Contacts

Erica Davis

Global Co-head of Cyber
Erica.Davis@guycarp.com

Jess Fung

Head of North America Cyber Analytics
Jess.Fung@guycarp.com

Additional Contributors:

Vadim Filimonov

Shu Iida

Richard McCauley

How Guy Carpenter Can Help

Guy Carpenter's global Cyber Center of Excellence is a dedicated team of brokers, product innovators and analytic experts advancing the role of cyber reinsurance and retrocession. We work closely with clients to share updates on the threat landscape, deliver cyber industry insights, construct relevant modeling scenarios, and design reinsurance placements to protect these portfolios.

GuyCarpenter

About Guy Carpenter

Guy Carpenter & Company, LLC is a leading global risk and reinsurance specialist with more than 3,400 professionals in over 60 offices around the world. Guy Carpenter delivers a powerful combination of broking expertise, trusted strategic advisory services and industry-leading analytics to help clients adapt to emerging opportunities and achieve profitable growth. Guy Carpenter is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. The Company's 83,000 colleagues advise clients in 130 countries. With annual revenue of nearly $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses including Marsh, Mercer, and Oliver Wyman. For more information, visit www.guycarp.com and follow us on LinkedIn and Twitter @GuyCarpenter.