GuyCarpenter

at bay

SMALL BUSINESSES AND THE NEW FRONTIER OF CYBER CATASTROPHE MODELING

A business of Marsh McLennan

Key Takeaways

- Small and medium businesses (SMBs) now represent 45% of the cyber market exposure, an increase of 45% over the last 5 years. The increased share of SMBs in the cyber insurance market makes accurate quantification of their aggregation potential critical to capacity deployment and risk management.
- Compared to the overall SMB segment, SMBs with cyber insurance coverage generally exhibit stronger security postures. This separates the security posture of such SMBs significantly from the general population, and it is very important to incorporate this security posture gap in cyber modeling analyses to accurately quantify the appropriate aggregation risk for the corresponding portfolio.
- Due to the lack of credible data, cyber catastrophe (CAT) models can struggle to reflect the disparities of cybersecurity postures in the SMB space. Adjusting CAT model outputs to reflect the impacts of fundamental security controls allows for more accurate and precise differentiation of SMB risks. Model adjustment is therefore a crucial step in establishing a robust view of modeled loss potential to support the growth in a market segment poised for continued expansion.
- An example of CAT model adjustment for SMB risks using At-Bay data shows a 17% reduction in CAT-only tail losses on the 250-year return period when multi-factor authentication (MFA) and endpoint detection and response (EDR) security controls are accounted for in the model.

The cyber insurance market has grown rapidly since its beginning, and cyber catastrophe (CAT) modeling is becoming an increasingly crucial tool for insurers and reinsurers to understand their cyber risk and determine how much cyber exposure to bear. The integration of cyber CAT models into cyber risk management decisions helps in quantifying these risks more effectively, deploying capital strategically and minimizing CAT exposure.

Initially, cyber insurance was designed for large businesses with complex network systems, which were prime targets of cyber attacks. Over time, however, threat actors and their tactics have evolved. Now, no business is immune from cyber risk. In fact, 98% of cyber claims from the last 5 years came from businesses with under USD 2 billion in revenue.[1] As a result, more and more small and medium-sized businesses (SMBs) are seeking cyber coverage.

SMBs have drastically different risk profiles than do large businesses. While cyber CAT models have matured and been adopted by many insurance and reinsurance companies in recent years, current cyber CAT models still struggle to adapt to SMB exposure.

The lack of historical data about technology adoption and security postures of SMBs makes it difficult for cyber CAT models to properly assess SMB cyber aggregation. For these reasons, further evolution of the cyber CAT model is necessary. In the short term, insurance and reinsurance companies can supplement data to vendor models and modify outputs to more accurately reflect the cyber CAT risk for the SMB segment.

In this paper, Guy Carpenter is joining At-Bay*—a leading InsurSec provider to SMBs—to explore the current limitations in the cyber CAT modeling of the SMB segment and to propose a way to adjust model output based on security control information.

Cyber CAT Modeling Plays a Crucial Role in Capacity Deployment

Cyber incidents have the potential to cause significant, widespread damage, necessitating careful management of aggregate limits exposure to ensure that insurers and reinsurers can cover potential losses without exceeding their capacity and stay within a predictable exposure. For example, WannaCry[2] impacted more than 200,000 computers globally through a vulnerability in Microsoft Windows in 2017. NotPetya[3] occurred in the same year and cost more than USD 10 billion globally. Most recently, the CrowdStrike Falcon outage affected 8.5 million Microsoft devices globally.[4] These events underscore the fact that cyber CAT events could happen at any time, and insurance companies have to understand the nature of cyber CAT and control its limits to protect their financial health.

CAT modeling is an important tool for capacity deployment, especially when addressing the potential for catastrophic losses associated with cyber risk. There is wide adoption of vendor models in the insurance and reinsurance markets for this purpose. Vendor models are essential in helping companies understand and quantify their exposure to cyber threats, enabling them to deploy their capacity more effectively. By leveraging these models, insurers and reinsurers can make informed decisions about how much and what types of risk they can adequately underwrite.

[1] NetDiligence, Cyber Claims Study, 2023 Report. https://netdiligence.com/wp-content/uploads/2023/10/2023-NetDiligence-Cyber-Claims-Study_v1.1.pdf
[2] NHS ransomware attack: what happened and how bad is it? The Guardian. https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it
[3] The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[4] Microsoft says about 8.5 million of its devices affected by CrowdStrike-related outage | Reuters

Cyber CAT models work by mapping interdependencies within a portfolio and measuring potential losses through simulations. These simulations consider various scenarios and interconnections, providing a comprehensive view of how a cyber event might impact different parts of a portfolio. This detailed analysis is crucial for understanding the potential aggregate impact of cyber risks and for developing strategies to mitigate these risks.

A CAT vendor model uses the underlying portfolio of a client to assess exposure to various scenarios by examining single points of failure (SPOFs). SPOFs are a key element of CAT models that connect specific CAT scenarios to companies. For example, geolocation is a key SPOF for natural catastrophe models (earthquakes, hurricanes, and so on). If buildings are close to specific fault lines, they will be impacted in the event of an earthquake. In cyber CAT models, common digital assets (software, services, and so on) are the key SPOFs because they form critical technology that can manifest into widespread events through cyber attacks. By identifying SPOFs, the cyber CAT models help insurers and reinsurers understand their vulnerabilities and develop plans to address them.

The vendor model often supplements the information provided by the client to get a more granular understanding of potential SPOFs and aggregation. This supplemental information is mostly detailed firmographic and technographic information. Especially for technographic information, model vendors traditionally use outside-in scans to collect information about internet-facing software.

Digital dependency on software, services and so on can be determined via a scanning engine. Cyber CAT models use that information to connect entities and create an understanding of the network. This supplemental information enhances the model's accuracy and provides a deeper insight into the client's specific risk landscape. By combining client data with advanced modeling techniques, insurers and reinsurers can achieve a more robust assessment of their exposure and make better-informed decisions about capacity deployment and risk management.

Evolving Cyber Threats Drive SMBs to Adopt Cyber Insurance as Attack Methods Shift

Large businesses were the earliest adopters of cyber insurance, driven by the risk of large data breach incidents (such as Target 2013, Home Depot 2014, Sony 2014, and so on). Threat actors traditionally targeted large businesses due to the sheer amount of sensitive data these organizations manage—typically yielding a large payout in a successful attack (e.g. Colonial Pipeline 2021, JBS 2021, and Caesars Entertainment 2023).

More recently, however, threat actors have begun to opt for more repeatable and scalable attack methods by exploiting vulnerabilities in popular technology products that are used by many businesses (e.g. ProxyShell 2021, Log4j 2022, and FortiGate 2023) rather than targeting specific organizations themselves. Ransomware has become a primary attack method, thanks to the potential for immediate financial gain via ransom payment and the anonymized financial transactions enabled by cryptocurrency.[5] To maximize efficiency, threat actors have begun to repeat the same ransomware attacks far and wide by reusing common entry points, which leads to cyber aggregation attacks.

Because this recent trend has threat actors targeting common entry points to maximize efficiency, the mainstream ransomware attack can be considered an opportunistic aggregation attack rather than a targeted attack. This opportunistic attack method increases the frequency of cyber claims by SMBs, compared to large businesses (67% of organizations impacted by ransomware in Q4 2023 were SMBs with fewer than 1,000 employees).[6] This, in turn, has led to more SMBs purchasing cyber insurance. **According to proprietary information from GC CyberExplorer® DataLake, SMB exposure was 31% of the total cyber market 5 years ago; today, it is 45%.**

SMBs Have a Wide Disparity of Security Postures

Increased cyber risk for SMBs has made SMB cybersecurity a key topic in cyber coverage. Security controls have been evolving at a rapid pace to match the progression of threat actors, and these modern security products have proved their ability to mitigate the impact of attacks.

Historically, simpler security gaps, such as open ports for remote desktop protocol (RDP), were the cybersecurity industry's focus, but the trend has shifted toward closing these once-common vulnerabilities. Today's cybersecurity landscape emphasizes more sophisticated and comprehensive risk controls. This includes the implementation of endpoint detection and response (EDR), extended detection and response (XDR), managed detection and response (MDR), and zero trust networks, among others. These advanced measures are pivotal in fortifying security perimeters against increasingly complex threats.

However, the cybersecurity environment for the SMB segment is worse than it is for large businesses. SMBs don't have a big enough security budget to employ enterprise-grade security products and services[5]—and

[5] Committee on Homeland Security and Governmental Affairs, Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security, US Congress. Senate.
[6] Coveware, Ransomware Quarterly Reports 2023 Q4, https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying

they often lack sufficient personnel to configure and manage them—which makes the SMB segment a less-attractive market for security providers.

Despite growing recognition among small businesses of the need to enhance their security measures, the reality remains that smaller businesses have access to fewer support resources compared to larger businesses. This access gap leads to a wide disparity of security postures within the SMB segment, with the 2 ends of the spectrum being those with and those without cybersecurity products and services.

Compared to the overall SMB segment, SMBs with cyber insurance coverage generally exhibit stronger security postures, particularly when they opt for security services provided either by reputable third-party security firms or directly through their insurance providers. This separates the security posture of small businesses with cyber insurance or cybersecurity significantly from the general population, and it is very important to incorporate this security posture gap in models to accurately quantify the appropriate cyber aggregation risk for the corresponding SMB portfolio.

Protecting SMBs from Cyber CAT Events: Strategies for Mitigating Widespread Malware Events

The main issue is that SMBs often lack in-house cybersecurity capabilities, making them more susceptible to certain types of aggregation events. Unlike larger businesses that typically have dedicated cybersecurity teams and robust defenses in place, SMBs mostly operate with limited resources and expertise in this area. This difference in cybersecurity preparedness means that the impact of various cyber scenarios can differ significantly between SMBs and larger businesses. Consequently, the weighting of risk scenarios needs to account for this susceptibility, potentially assigning different risk levels to SMBs based on event scenarios and their internal security postures.

Cyber CAT events are a distinct category of cyber aggregation events characterized by their automated and scalable nature, which allows them to impact multiple organizations through a single event. Given SMBs' lack of in-house cybersecurity capabilities, widespread malware is one of the CAT events impacting SMBs more than large businesses, which is automated malware that propagates into organizations' networks via common entry points and impacts those organizations without any human intervention.

Understanding the mechanics of these attacks is vital for developing effective defense strategies. The cyber kill chain[7] serves as a critical framework for deciphering the stages of a cyber attack, allowing organizations to better anticipate and disrupt potential threats. By dissecting this sequence, organizations can implement targeted security measures at each stage to mitigate the impact of attacks. The following section outlines the typical sequence of malware attacks, providing an in-depth look at each stage and the strategies employed by cybercriminals. Additionally, it explores the security controls that are effective to prevent and mitigate the effects of widespread malware events.

The Malware Attack Sequence

The cyber kill chain is a framework for understanding the sequence of stages cybercriminals take in an attack. The following is the typical sequence of malware attacks:[8]

1. **Reconnaissance and target selection:** Researching and selecting organizations with potential entry points to attack.
2. **Initial infection:** Gaining initial access to a targeted organization's network.
3. **Lateral movement and privilege escalation:** Malware propagation within a targeted organization's network to reach important digital assets.
4. **Encryption, destruction and/or data exfiltration:** Encryption or deletion of important digital assets and/or stealing sensitive information.
5. **Extortion and negotiation:** Demanding ransom payment and negotiating with the targeted organization.
6. **Recovery and mitigation:** Restoring systems and encrypted data and mitigating the risk of future attacks.

In cyber CAT events, malware is widely distributed automatically—without human intervention— through vulnerabilities in public-facing software, software update mechanisms or managed service providers (MSPs). The process typically leverages the attack sequence in order. In this way, malware can impact many organizations at once without resource constraints. For organizations to prevent and/or mitigate the impact of widespread malware, the malware has to be stopped before the impact is materialized in stage 4 (encryption, destruction, and/or data exfiltration).

Security Controls to Mitigate the Risk of Widespread Malware

Organizations protect their networks against cyber attacks by implementing security controls such as firewalls, EDR, MFA, backups, etc., and adopting a defense-in-depth strategy with security layers. Security controls in each layer can work efficiently against widespread malware by stopping each stage of the attack. MITRE ATT&CK[9]

[7] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, Leading Issues in Information Warfare & Security Research, vol. 1, no. 1, p. 80, 2011.
[8] Flashpoint, The Seven Phases of a Ransomware Attack: A Step-by-Step Breakdown of the Attack Lifecycle, https://flashpoint.io/blog/the-anatomy-of-a-ransomware
[9] MITRE, ATT&CK Matrix for Enterprise, https://attack.mitre.org

Table 1: Security Layers Associated with Security Controls

Security Layer	Major Security Controls	Ransomware Attack Sequence
Network and Perimeter	VPN, firewall	Reconnaissance and target selection / initial infection
Endpoint	EDR	Initial infection / lateral movement
Application	MFA	Lateral movement
Data	Backups	Extortion and negotiation

Source: At-Bay

provides the relationship between the stages of the attack lifecycle, adversary tactics that map to each stage, and corresponding defensive countermeasures. The summary of security controls associated with each security layer is as follows.

- **Network layer and perimeter layer:** These layers protect the network against malicious intrusion. Security controls, including virtual private networks (VPNs) and firewalls, work to prevent malware delivery.
- **Endpoint layer:** This layer secures individual endpoints including servers, workstations, and laptops via security controls including EDR, which can stop the initial infection effectively. EDR is designed to protect endpoints automatically and send alerts, isolating potential threats by detecting the malicious behavior of malware. A recent ransomware claims investigation shows the importance of EDR and its configuration:[10] EDR must be implemented properly to all endpoints with the appropriate configuration, otherwise it may be ineffective in preventing malware. This is why MDR, which includes a security team to manage the EDR solution, is the ideal option for most businesses (especially SMBs) that lack the IT resources or technical capabilities to effectively implement and maintain these systems on their own.
- **Application layer:** This layer secures access to applications by security controls, including MFA. Network segmentation is very effective in stopping lateral movement; however, proper access control is required to allow only necessary access to segmented networks. This protection can effectively inhibit lateral movement.
- **Data layer:** This layer protects sensitive data via backups. In the case that important digital assets are encrypted or deleted by malware, it's essential for businesses to implement robust backups and maintain their quality. Backups do not stop malware, but they help with faster system recovery and provide an alternative to paying a ransom to access encrypted data.

Since ransomware has to be stopped before encryption or exfiltration of data to mitigate the impact, protecting network and perimeter, endpoint and application layers is an effective way to mitigate the risk. Modeling the security controls associated with those layers is an important next step to assess cyber risk properly in the cyber CAT model. However, modeling the security controls in endpoint and application layers is one of the challenges for model vendors due to the lack of visibility from the public internet.

The Challenges of Assessing SMB Aggregation Risk

To support the need to understand the total aggregation potential of automated and scalable events, the cyber insurance industry must be able to accurately quantify the risk presented by a growing SMB segment. Cyber CAT models have matured over the last 10 years and have been adopted by the insurance industry as part of cyber risk management. However, there are still challenges in assessing cyber CAT risk for the SMB segment given the strong heterogeneity of cybersecurity posture due to budget and resource constraints, as well as the evolution of security controls.

Challenge 1: Lack of incident data

There is not much data for cyber CAT, since these events are rare by definition. However, we can learn the behavior of companies in non-CAT cyber incidents data, since cyber CAT can be considered correlated with non-CAT cyber events. Although there is more incident data available for large businesses, there is not enough publicly available information on historical incident data since attacks on the SMB segment are only a recent trend. Also, due to the lack of government regulation mandating the disclosure of ransomware incidents, there is less motivation to report/publish incidents publicly, especially for SMBs. Insurance companies gradually accumulate claims information and publish the insights.[11] [12] [13] However, model vendors don't have access to detailed claims information.

[10] Comcast Business, How Endpoint Detection and Response (EDR) Can Help Reduce Serious Incidents, https://business.comcast.com/community/browse-all/details/how-endpoint-detection-and-response-edr-can-help-reduce-serious-incidents

[11] At-Bay, The 2024 InsurSec Report: Ransomware Edition, https://www.at-bay.com/2024-insursec-report/

[12] Coalition, The State of Active Insurance: 2024 Cyber Claims Report, https://www.coalitioninc.com/blog/2024-cyber-claims-report

[13] Cowbell, Cyber Round-Up: Q2 2023, https://cowbell.insure/wp-content/uploads/pdfs/Cowbell-Cyber-Round-Up-Q2-2023-1.pdf

Challenge 2: Lack of credibility in public data

While some data vendors provide incident data, its reliability is questionable. Ransomware is a complex and dynamic issue that requires understanding the interaction between threat actors, attack vectors, attack surfaces, security controls, and human resource components. Simply knowing the number of incidents is insufficient to grasp ransomware trends comprehensively. Lack of detailed information leads to coarse resolution of the model. As mentioned before, cybersecurity for SMBs is dynamic and heterogeneous. Without having reliable, detailed information, it is difficult to build models to assess SMBs. Additionally, datasets likely contain unknown amounts of false negatives due to the reasons mentioned above. Skewness and bias in the data have to be handled well to avoid biased output. Insurance claims are the most accurate data source, but model vendors typically lack direct access to this information.

Challenge 3: Insufficient SMB information

The cyber CAT model initially focused on data breach incidents of large businesses, as this was the primary concern when cyber insurance began. However, as threat actors have shifted their tactics, the modeling focus has expanded to include SMBs. Despite this shift, vendor models still struggle to collect sufficient data on SMBs. On top of that, the technological dependencies within their networks are not obtainable from outside-in scans. Potentially, this type of information can be supplied by insurance companies; however, most insurance companies don't gather this data. This makes it difficult for model vendors to implement technological interdependencies and difficult to understand the interdependencies within this segment. Moreover, some models assume "market share" tech stacks based on enterprise data, which grossly misrepresents the unique technological profiles of SMBs. With over 30 million SMBs in the US alone,[14] covering all companies in each insurance portfolio remains a significant challenge.

Challenge 4: Interdependencies in SMBs

Interdependencies are particularly critical in the SMB segment, where security controls are often less robust compared to larger businesses. SMBs tend to rely heavily on critical infrastructure and third-party software services, making them especially vulnerable to widespread disruptions. Due to their weaker security controls, a breach in one part of the critical infrastructure or software ecosystem can have a cascading effect, significantly impacting multiple SMBs simultaneously. Traditional risk models do not have comprehensive data on SMB interdependencies and often fail to understand the intricate network relationships and their impact. Therefore, it is essential to enrich datasets with detailed information about these interdependencies and to thoroughly understand their potential financial impact.

Supplementing Data to Vendor Models and Modifying Outputs to Accurately Reflect SMB Portfolios

To overcome the lack of SMB information, especially for security controls, we propose this methodology to compute the losses with the security control information provided outside of the model. By overlaying the impact of the security controls on the loss output of the vendor CAT model, we can have a better understanding of cyber CAT in the SMB segment.

EDR and MFA are fundamental security controls inside the network for protecting SMBs from malicious attacks, as described in the previous section. Many claims occur because of a lack of EDR and MFA or a lack of proper configuration. However, the security controls associated with security layers inside the network are not yet modeled well in cyber CAT models due to the lack of security control data.

The absence of this data stems from the limitation of outside-in scans and the lack of incident data connecting the evolving security controls to real-world cyber incidents in a timely manner. In the short term, overcoming these challenges can be achieved by supplementing data to vendor models and modifying outputs to more accurately reflect SMB portfolios.

Incorporating the effects of EDR and MFA into the cyber CAT model enhances our understanding of cyber risks, particularly in the Endpoint and Application layers. These controls are vital as they can pre-emptively halt ransomware attacks before they cause significant damage. However, considering the wide range of security postures among SMBs in the insured portfolio, it is essential to factor in the existing security controls within these organizations' networks when modeling the cyber risk for SMBs.

- **EDR** has evolved in recent years, and now it can work efficiently against both known and unknown malware via behavior blocking. By isolating malicious malware, EDR stops malware before it impacts the network. EDR can also increase the investigation/recovery speed via systematic data collection in case of any compromisation.

- **MFA** plays an important role in network segmentation to allow only legitimate access between network segments, which can stop lateral movement by limiting malware's impact on small network segments even in the case of

[14] US Chamber of Commerce, The State of Small Business Now, https://www.uschamber.com/small-business/state-of-small-business-now

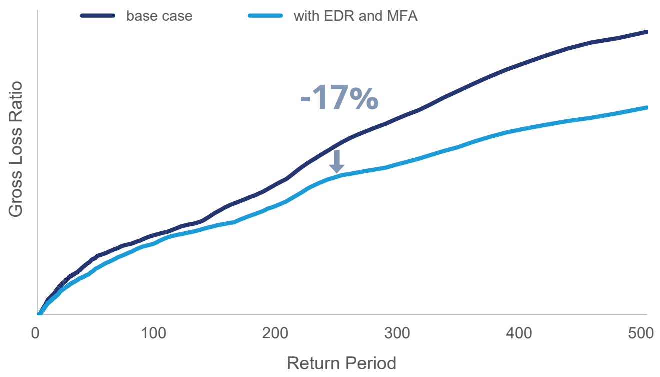
successful network infection. Without lateral movement, the likelihood of important digital assets being compromised is significantly lower.

Insurance companies have to accommodate the impact of security controls in cyber CAT assessment for the SMB portfolio via their own or vendor models. In this paper, we illustrate how At-Bay does this on its own portfolio of policies placed through At-Bay by using a vendor model. At-Bay relies on outside-in data, inside-out data, and self-reported information to collect data throughout the policy period for each insured. Because neither EDR nor MFA are easily visible from the public internet, both inside-out and questionnaire data are essential. Understanding insureds' security posture throughout the policy period is crucial for cyber risk assessment due to the dynamic nature of cybersecurity.

Based on the security posture observed for insureds with policies placed through At-Bay, the simulation level of ground-up losses is adjusted from a cyber CAT model output. First, the size of the footprint per simulation is reduced based on the proportion of the insureds with EDR. Next, the severity of the claims is reduced for the insureds with MFA by preventing lateral movement and/or EDR by increased recovery speed based on At-Bay's claims analysis.

The below aggregate exceedance probability (AEP) curves for the gross loss ratio are computed based on the in-force portfolio of policies placed through At-Bay as of December 2023. It shows the impact of EDR and MFA on CAT-only tail losses. The effectiveness of these security controls is more limited below 100-year return periods, as widespread malware events contribute less significantly in these intervals. However, in the 250-year return period, the impact of these controls is more pronounced, resulting in a 17% reduction.

Figure 1: Aggregate Exceedance Probability Curves Based on Gross Loss Ratio



Source: At-Bay

Conclusion

The insurance industry must take into account the small businesses that make up the backbone of the economy in order to support continued, long-term growth. However, SMBs are not well modeled in cyber CAT models due to challenges this segment faces that are different from large businesses, as described above. Without a better understanding of cyber CAT risk, it might be harder to attract capital at scale in the SMB segment.

In terms of the cyber threat landscape, ransomware incidents have become more opportunistic in recent years as threat actors take advantage of common entry points, impacting organizations of all sizes. This has led to increased risk for SMBs, since these organizations typically have greater variability in security postures due to smaller IT budgets and limited in-house expertise. Because internal security controls significantly improve SMBs' security postures, it is crucial to incorporate them into the cyber CAT model to quantify risk exposure appropriately.

Current vendor CAT models have been playing an important role in the capital allocation decision process; however, it is not easy to apply to the SMB segment due to the lack of information in many aspects, including incidents, firmographic information, technographic information, outside-in and inside-out data. Detailed inside-out information has to be provided by insurance companies and overlaid on the model output to create a better assessment of SMB cyber CAT risk.

In this paper, we propose a framework of how modelers can improve vendor model accuracy, and showed examples on At-Bay data for 2 security controls (EDR and MFA). The adjustment modifies the ground-up loss simulation per policy and can be applied to any vendor model. The impact of EDR and MFA on the return period gross loss ratio is observed to be significant. The return period losses in the tail (e.g. 100, 200, 250 years, and more) are typically used by most carriers to manage their balance sheet. In the case of At-Bay's portfolio as of December 2023, the 17% reduction in the 250-year return period indicates that the gross loss ratio could be even lower if more organizations in the portfolio were to acquire security controls.

In order to allocate capital efficiently, the insurance industry needs to improve its understanding of cyber CAT risk in SMB portfolios. It is imperative to deepen our understanding of internal security controls within the defensive aspect of cyber risk and their limitations. More importantly, a precise understanding of interdependencies is required. Granular representation of SMB portfolios will enable cyber CAT models to reflect risk accurately and allow the insurance market to expand more confidently in the SMB segment, where rapid growth is expected to continue in the future due to increasing technological reliance.

Authors

Jess Fung, Managing Director and North American Cyber Analytics Lead at Guy Carpenter

Richard McCauley, Vice President and Senior Cyber Catastrophe Advisor at Guy Carpenter

Emma Ye, Vice President of Risk at At-Bay

Yoshi Yamamoto, Cyber Risk Modeling Director at At-Bay

About Guy Carpenter

Guy Carpenter & Company, LLC is a leading global risk and reinsurance specialist with 3,500 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 more than 85,000 colleagues advise clients in over 130 countries. With annual revenue of $23 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 X.

About At-Bay

At-Bay is the insurance provider for the digital age. By combining world-class technology with industry-leading insurance, At-Bay was designed from the ground up to empower businesses of every size to meet cyber risk head on. At-Bay Insurance Services, LLC provides insurance protection and security prevention solutions to close to 40,000 businesses in the US, safeguarding up to $800B in collective business revenue, and offers coverage by admitted and non-admitted insurers for Cyber, Technology Errors & Omissions (Tech E&O), and Miscellaneous Professional Liability (MPL). The At-Bay Group also includes an active full-stack insurance company and a cybersecurity company. At-Bay Security offers proprietary security solutions including At-Bay Stance Managed Detection & Response (MDR).

*All statements for At-Bay, Inc., companies.

The information contained in this document is intended for general informational purposes only and is not intended to provide legal or other expert advice. You should consult knowledgeable legal counsel or other knowledgeable experts as to any legal or technical questions you may have. Neither At-Bay nor its employees shall be liable for the use of any information or statements made or contained in any information provided herein.

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. 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. The trademarks and service marks contained herein are the property of their respective owners.