WHITE PAPER

2025 US Cyber Industry Exposure Database and Loss Curve

A collaboration between Guidewire Cyence and Guy Carpenter

The cyber landscape has been rapidly changing throughout 2025. US federal deregulation and defunding of key cyber agencies, nation-state cyber activity and ongoing foreign wars: these developing conditions create new uncertainty, and present new opportunities for cyber attackers to capitalize on the uncertainty.

For example, recent reductions in US federal oversight over security standards for large cloud providers presents the opportunity for such providers to decrease resource allocation toward security protocols or vulnerability remediation, both previously standard practices in the industry.

Nevertheless, large cloud providers may also benefit from any newly freed resource, potentially accelerating R&D velocity with fewer regulatory obligations. It is entirely possible that this improved velocity on network security innovation would outweigh the vast reduction of federally established protocols. However, the ultimate impact of these procedural adjustments cannot easily be measured: in all likelihood, deregulation impacts on security will overtake efficiency benefits, at least in the short term. Therefore, it can be considered that the general 2025 cyber industry landscape is at a higher risk level than in 2024.

In response to this tumultuous moment in time, financial and insurance markets require a fresh estimate of industry cyber exposure. In this spirit, Guidewire Cyence (Cyence) and Guy Carpenter (GC) are releasing a newly constructed, fully unique and up-to-date **US Cyber Industry Exposure Database and Loss Curve (IED).**

The IED satisfies a number of use cases, including market exposure measurement, aggregation benchmarking, data supplement and support, and various risk transfer vehicle calculations. Cyence and GC plan to maintain this collaboration with regular updates, new version releases and additional functionality for the IED product beyond 2025, including the expansion from US to a global view. This paper will explore Cyence and GC opinions on market conditions, showcase IED statistical outputs, and provide a step-by-step walkthrough of our IED build logic.

We abide by the principle of full transparency: a single numerical curve without insight into its construction should not be sufficient justification to trust a model. Thus, our goal with this paper is to encourage deeper discussions not only on the technical findings, but also any potential areas for improvement in future iterations, to garner trust and comfort in our collaborative solution. We look forward to this discussion.

Table of Contents

The opening sections of this paper capture the main findings of the IED project and the general cyber landscape opinions shared across GC and Cyence. Readers who wish to examine IED build details can refer to the sections under "IED Methodology Detail." Finally, we provide a preview of future IED iterations for successive Cyence model versions.

Executive Summary and IED Results

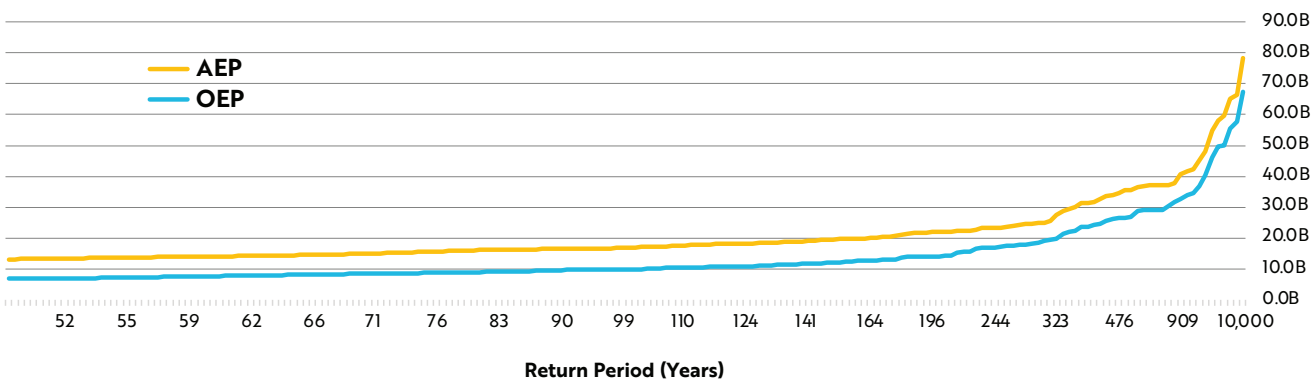
As expounded upon later in the "Define IED Form and Scope" section, an Industry Loss Curve is fundamentally an ascending curve of possible extreme cyber loss scenarios, each assigned a unique likelihood. In this case, the Cyence and GC loss curve results include sets of both the largest event per simulation years ("Occurrence Exceedance Probabilities" or "OEP"), and total annual loss years ("Aggregate Exceedance Probabilities" or "AEP"). Other cyber risk metrics are also included in the analysis, but some high-level benchmark statistics from our analysis can be summarized as follows:

		US Cyber Market Insurance Results ($B)		
		Per Occurrence	Annual Aggregate	Note
(a)	1-in-100 Loss	9.94B	16.53B	
(b)	1-in-250 Loss	17.23B	24.42B	Direct IED model output
(c)	Expected Loss		5.05B	
(d)	Projected US Annual Written Premium		9.52B	Census * Takeup Rate * Avg. WP per policy
(c)/(d)	Projected US Cyber Industry Loss Ratio		53.0%*	Insured Loss (post-retention/attach/limit) / Standalone + Package Annual WP

- Loss estimates from Cyence Model version 7: Premium statistics provided by GC
- Estimated count of US Cyber Policies (primary): 4.97 million
- Manufacturing, Financial Services and Retail Trade sectors have the largest presence in extreme tail events
- 12 month in-force affirmative cyber exposure data for analysis as of Q4 2024

**53% loss ratio is composed of attritional loss (42 percentage points) and cat loss (11 percentage points)*

OEP and AEP VaR (Value at Risk) curves



			OEP			
RP	**AEP**	**Loss Ratio**	**Dollars**	**Counts**	**Event Set**	**Provider**
Max	78.3B	823%	67.3B	436,520	Mass Ransom	Windows
1 in 500	36.5B	383%	26.6B	210,878	Mass Ransom	Windows
1 in 350	30.1B	316%	22.0B	172,473	Mass Ransom	NGINX
1 in 250	**24.4B**	**257%**	**17.2B**	**141,729**	**Mass Ransom**	**Windows**
1 in 200	**21.6B**	**227%**	**14.1B**	**147,922**	**Mass Ransom**	**Apache**
1 in 175	19.8B	208%	13.2B	478,991	Cloud	Xen
1 in 150	19.3B	203%	12.2B	176,683	Mass Ransom	Windows
1 in 100	**16.5B**	**174%**	**9.9B**	**174,765**	**Mass Data Breach**	**Windows**
1 in 75	15.5B	163%	8.7B	95,708	Mass Ransom	Windows
1 in 50	13.2B	139%	6.8B	144,626	Mass Data Breach	Windows

OEP and AEP simulated years are individually ordered in the line chart (top).

Across 10,000 simulation years, the largest 200 loss years represent the 1-in-50 return period and beyond.

Feasibility of a 1-in-100 174% US Gross Loss Ratio Result

The return period table above represents modeled losses derived from the Cyence Model 7.1 US IED industry loss curve. At the 1-in-100 return period level, it suggests a 174% US-industry wide aggregate loss ratio. This particular simulation year is composed of 69 loss ratio points of attritional (non-cat) accumulated loss, with the remaining 105 points stemming from a single cat event of $9.9B. This 69% attritional loss ratio is higher than Cyence modeled expectation for the upcoming policy year of 42% (refer to note in Executive Summary, page 3). However, this 1 in 100 tail return period result is intended to reflect a worse than average policy year; one that is still well within reasonable possibility, especially considering the high cyber industry loss ratio experience in 2019 and 2020.

The following sections go on to support the feasibility of the cat portion of this simulation via a relative comparison to the known and now fully developed NotPetya event of 2017.

Comparison to NotPetya

- This is the largest insured cyber event in history (2017) at an estimated insured loss of $3B* (approaching $4B in 2025 terms). This size of event falls between the 1-in-10 and 1-in-20 return period on the Cyence IED OEP curve. From this loss perspective, an insured industry event of approximately 2.5 to 3 times the size of NotPetya ($9.9B) would be required for the industry's annual aggregate loss ratio to reach a 174% level under current premium and coverage conditions, along with the elevated level of attritional loss ratio of 69% discussed above.

**https://www.verisk.com/4a25ed/siteassets/media/pcs/pcs-cyber-catastrophe-notpetyas-tail.pdf*

- Despite being the most economically damaging cyber event in history, NotPetya impacted only 2,300 businesses worldwide, primarily focused on Ukrainian businesses, given the initial backdoor for entry was a regionally used tax-management software mostly unique to Ukraine (M.E. Doc). Additionally, only a single EternalBlue vulnerability vector was utilized in the attack, and active data-destruction was not actually written into the malware code.
- Thus for several reasons, we can infer that a far more widespread and destructive version of NotPetya could have occurred within reasonable plausibility. If the scope of initial vulnerability were much wider (software vulnerability across US region, for example), the potential for impacted company counts could reach tens or hundreds of thousands — many multiples greater than the 2,300 businesses impacted in NotPetya.

Fallout of a 1-in-100 174% Loss Ratio Result

- From a rate environment standpoint, GC would expect the impact of a 174% industry loss ratio to result in a rapid hardening of cyber rates. This is based on history, during which cyber rates broadly increased in double- or triple-digit range following heightened loss ratio years in 2019-20. When we look at the loss performance of GC clients in those years, the group average was only in the 70-80% range by comparison. The 90th percentile client did not have a loss ratio higher than 150% in those years, yet we still observed the market materially hardening.

- Several dynamics in the cyber market changed following the peak loss ratio years of 2019-20. There was more cautiousness in terms of capacity deployment, more scrutiny of coverage level sublimits, an increase in policy attachment/retention requirements, and stronger focus on the insured's cyber security control and hygiene. All these measures were applied to re-establish a level of portfolio profitability and rate adequacy. We would expect a 174% loss ratio year to lead to similar outcomes.
- If the cyber insurance industry enters a heightened loss ratio environment, carriers could be expected to shift toward a more conservative buying behavior. Demand for quota share reinsurance would expand, as it provides an effective way to mitigate basis risk. Supply of proportional reinsurance capacity could continue to be available at the appropriate terms and conditions.
- Even in a year when the industrywide loss ratios reach unprecedented levels, the type of losses underlying such heightened loss ratio would lead to different appetite for reinsurance protection needs. If a 174% loss ratio is heavily cat-driven, carriers would naturally look to protect their balance sheets against the extreme volatility introduced by cyber cat occurrences. Cat event excess of loss (XOL), hybrid cat XOL + aggregate stop loss (ASL) structures, or alternative capital solutions including cyber cat bond, Industry Loss Warranty (ILW) and parametric covers may rise in popularity. On the other hand, while extremely unlikely, a 174% loss ratio year could arise from a multitude of independent non-cat losses. In that instance, more comprehensive risk-transfer solutions such proportional reinsurance and aggregate covers would become more appealing to carriers.

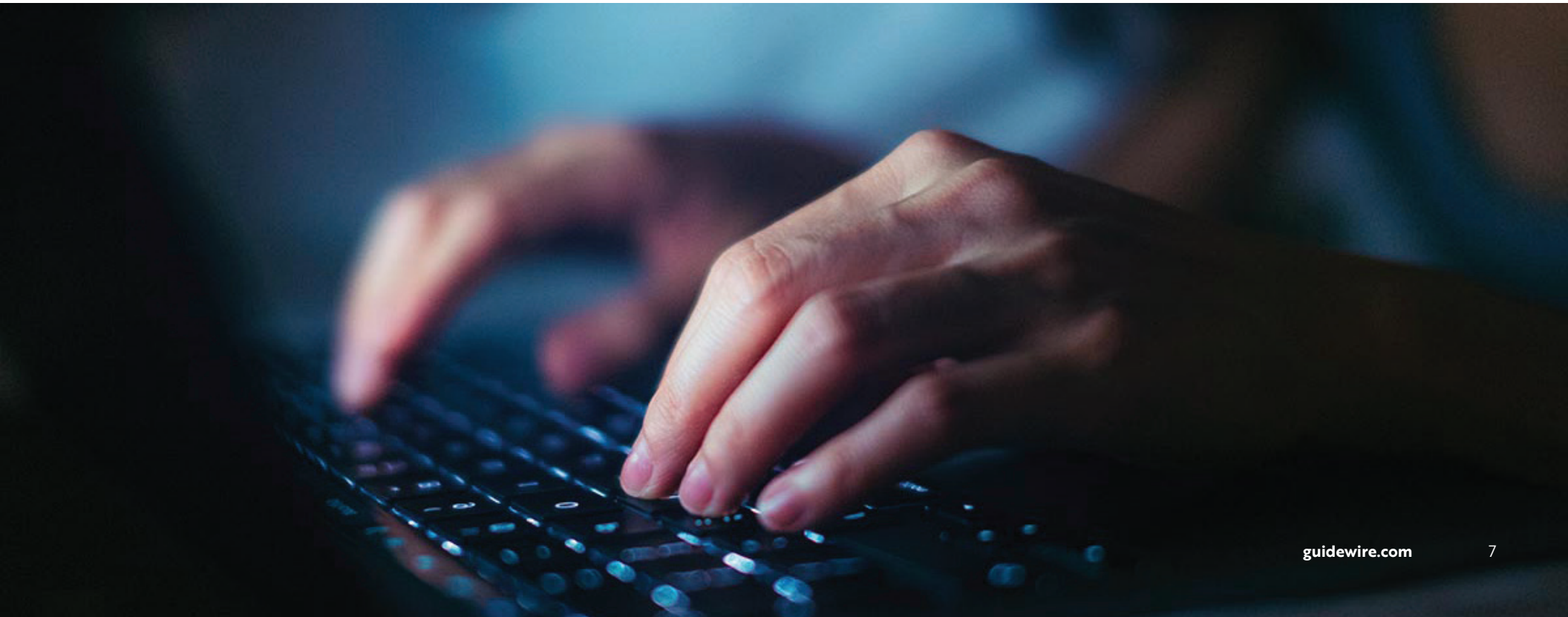
Impacted Counts

- Company counts per event are not monotonic, as events move into the tail. This is because total cat event losses are driven by average duration of provider outages and vulnerability exploits, certainly when large or mega-sized firms are materially impacted. Extended event duration against large firms will eclipse even vast numbers of affected small risks in many cases.
- We do not allow for all observed users of a particular software to be simultaneously impacted by a mass malware software-vulnerability exploitation event. Cyence asserts the existence of a maximum threshold of lateral spread for impacted organizations during such events, due to rapid and coordinated cybersecurity response measures:
  - Empirical evidence suggests that the propagation rate of malware significantly diminishes after the initial 12 to 24 hours following the onset of mass-scale cyber incidents, reflecting the swift implementation of containment protocols by affected enterprises and coordinated global cyber incident response teams.
  - Additionally, the global Chief Information Security Officer (CISO) community plays a crucial role by synchronizing their mitigation efforts, actively sharing threat intelligence and orchestrating collective defensive strategies.
  - Time-zone variations further influence this dynamic, as geographically dispersed organizations sequentially engage in remediation activities, creating a continuous response cycle that curtails the malware's overall propagation potential.

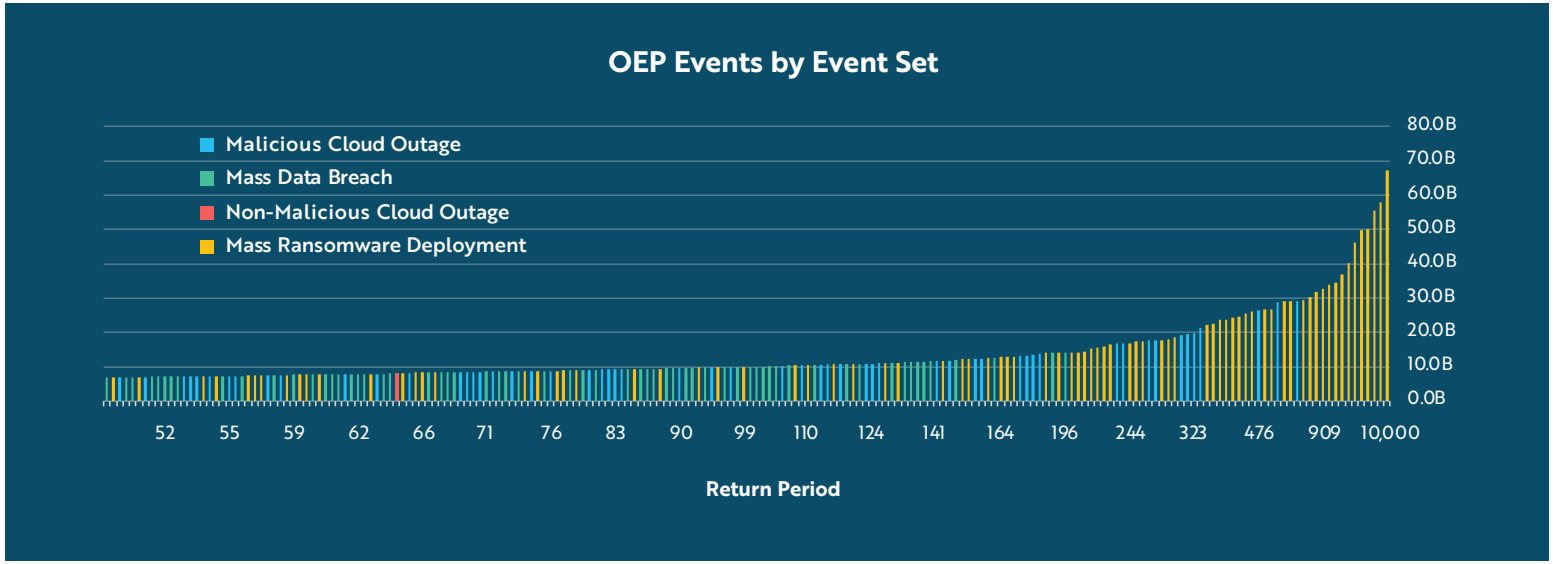
- Thus in terms of the IED model, these mitigating factors each imply that global vulnerability events will not reach all users of a given software, due to the containment efforts described above. Without recognizing these communal efforts to contain mass vulnerabilities, our tail results would potentially be overstated by magnitudes beyond realistic scenarios.

For further context

- Across all cyber client data GC has collected, only 25 out of 893 portfolio-years (3%) have a historical ultimate loss ratio over 174%. The most recent such occurrence was in 2022, when 1 portfolio out of 87 that year had an ultimate loss ratio exceeding that threshold. Therefore, the 174% loss ratio modeled by Cyence IED has, in fact, been observed in actual cyber writers' claims history, though only on individual portfolio bases.
- All GC portfolios observed with loss ratio years >174% continue to be viable. So, while each was certainly an earnings event for a particular year, none to date have reached the level of a capital event that threatened the solvency of a company or would cause them to withdraw from writing business.



Tail Composition by Event Type



The Mass Ransom deployment events occupy the majority of the very extreme tail, for several reasons:

- Highly effective malware can have correlative effects across impacted businesses and may possibly leave no option for internal backup.
- Successful ransom malware deployment is more achievable than the compromise of countrywide cloud provider services, which have many layers of redundancies in place.
- Ransom malware has high individual business severity potential, due to long duration curves (observed incidents reflect interruptions up to 120 days) — far longer than observed cloud provider outages. These differences are thus modeled accordingly:

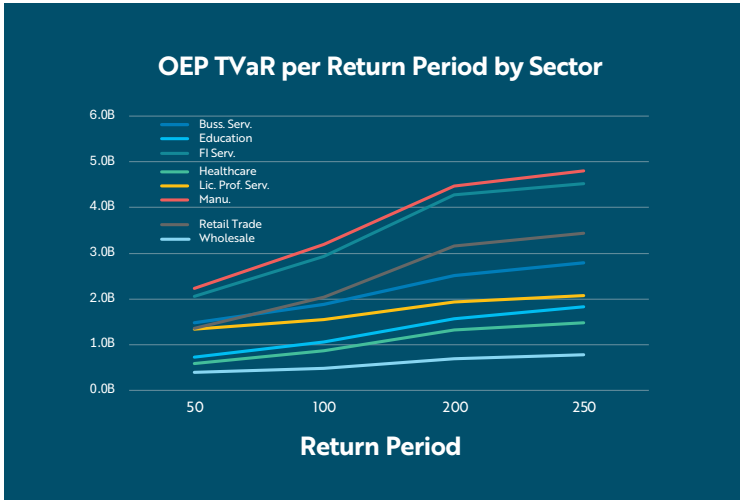
Days of Outage Duration in IED Events (1 in 50 +)

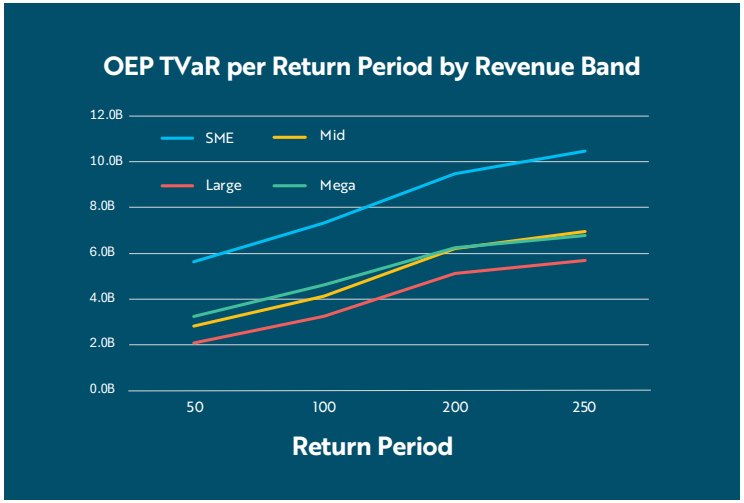
	Min	Average	Max
Software Vuln.	6.80	36.84	96.23
CSP	4.57	9.79	26.26

- The level of robustness and cyber security redundancies deployed by the major cloud service providers contribute to their relative lower presence in our IED tail losses when compared to large mass malware events. Major cloud provider services are also generally regionally deployed — thus, it is reasonable to assume a mass malware deployment via an internationally used software to be potentially harder to contain.
- Non-malicious cloud provider outages are seen more frequently than malicious attacks, but are modeled with an assumed shorter event duration, versus an equivalently dispersed malicious attack. Most modeled tail-contributing non-malicious events thus fall within the 1-in-50 OEP return period and shorter, when ordering events by loss magnitude.

Tail Value at Risk (TVaR) Stats

TVaR statistics are useful for observing the shifts in general composition of catastrophic years as the tail return period increases. Below, we display the relative composition of the tail by average risk size and industry sector:





OEP TVaR	Return Period			
Sector	50	100	200	250
Buss. Serv.	1.48B	1.88B	2.52B	2.80B
Education	0.73B	1.05B	1.56B	1.83B
FI Serv.	2.05B	2.93B	4.27B	4.52B
Healthcare	0.59B	0.87B	1.32B	1.47B
Lic. Prof. Serv.	1.33B	1.55B	1.93B	2.07B
Manu.	2.23B	3.20B	4.47B	4.80B
Retail Trade	1.35B	2.04B	3.16B	3.43B
Wholesale	0.39B	0.48B	0.69B	0.77B
Other	3.61B	5.26B	6.98B	8.02B
Total	13.75B	19.25B	26.90B	29.71B

OEP TVaR	Return Period			
Revenue Band	50	100	200	250
SME	5.63B	7.30B	9.45B	10.43B
Mid	2.81B	4.12B	6.17B	6.91B
Large	2.08B	3.25B	5.08B	5.65B
Mega	3.23B	4.59B	6.20B	6.72B
Total	13.75B	19.25B	26.90B	29.71B

TVaR by Sector

Manufacturing and Financial Services ascend most steeply into tail contributions, given high relative interruption duration due to physical systems (Manufacturing) and high average net income per unit time (Financial Services). These sectors also represent the majority of the largest risks in the world.

TVaR by Revenue Band

- Small to Medium-Size Enterprises (SMEs) comprise the majority of loss for the largest tail events.
- Given that the majority of tail events are Mass Ransom deployment, the heightened potential for outage duration means that large- and mega-sized firms will continue to contribute material sums to losses, in order to match the count volume that SMEs contribute to the loss.

Full 2025 Cyber Risk Landscape Commentary

As alluded to above, there is volatility in the current cyber risk landscape. The volatility encompasses all sectors and sizes of businesses, as well as all targeted and mass attack strategies. Ransomware and Business Email Compromise (BEC) attacks remain persistent into Q1 2025, and, in fact, reflect a material frequency increase compared to Q1 2024. For BEC at a minimum, this increased activity can be attributed traceably to new developments in AI attack sophistication: phishing messaging previously recognizable as external-party or bot-generated is now far more indistinguishable from trustworthy senders. We expect BEC attack frequency to increase at least in the short term, as AI penetrates the attack landscape, while security providers inevitably lag in implementing countermeasures.

Cyber modelers and financial markets are all monitoring the conflict in Ukraine. This conflict has consistently consumed economic and cyber attacker resources from both Russia and Ukraine for the better part of three years. If this conflict were to end in 2025, significant amounts of cyber-attack resources could be freed up to potentially renew attacks against other wealthy/insured nations. This resource shift can mean increased attack attention paid to wealthy targets for ransom, as opposed to targeted disruption for political gains. Furthermore, if US/Russia political tensions instead deteriorate over the next year, the US could expect heightened nation-state backing for potential attacks against US providers. Cloud hosts such as AWS have very regionally-divided service areas: even though some provider networks span across international business operations, a nation-state funded disruption against AWS hubs in the US would result in proportionally far more damage to US targets than for other nations, to the point that any potential blowback would not deter an attack from the aggressor country.

Of course, other geopolitical tensions beyond the Russia/Ukraine conflict are also of concern. For example, situations related to the potential deterioration of US/China relations, or the continuing tensions between China and Taiwan could heighten politically-driven cyber activity between the US and East Asia.

From another perspective, the commercial world is becoming more and more reliant on SaaS/PaaS 3rd-party providers to run their digitally connected operations. Thus, we have seen multiple single point of failure "cat" events over recent years (CDK Global, Change Healthcare, CrowdStrike, PowerSchool), which have often an industry-sector-localized impact, with potentially high severity. Many of these single points of failure (SPOFs) are hosted via established cloud providers, such as Google Cloud or Microsoft Azure — but the assumption that Google Cloud or Azure network security measures are sufficient to fully protect the hosted businesses themselves is a misconception. SPOFs, such as PowerSchool, must still work to maintain their own network security via user access management, managing backups and encryption, employee training and other various forms of security monitoring.

The other major cyber market shock the world is watching is the defunding of federal cyber security programs in the US. CISA

(Cybersecurity and Infrastructure Security Agency) provides continuous state threat intelligence to the US government and assists in curating KEVs (the Known Exploited Vulnerabilities catalog). This program has been reduced by $10M in annual funding, and approximately 10% of its workforce. FedRAMP (Federal Risk and Authorization Management Program) is a group that ensures cloud-based servers relied upon by the US government remain at acceptable standards for maintaining national digital security. The initiative to pursue AI-related measures has been scrapped in 2025— and cloud-usage authorizations have been reassigned to the private sector, away from slower moving (yet more closely monitored) central federal oversight.

To date, the magnitude of these various market forces is yet to be seen, but all elements point toward a more loosely regulated, potentially less secure digital environment for both US businesses and the US government.

Methodology Detail

A) Define IED Form and Scope

Characteristics of the IED project can be categorized as follows:

 Defining Properties	 Methodology	 Output
US Cyber-Insured Population	Independent Cyence Loss + GC Exposures	US Cyber Industry Loss Ratio + Written Premium Estimate
Cyence Model Version 7	"Bottom-up" Model Approach	OEP / AEP per sim year, beyond 1 in 50 RP
GC Exposure Data as of Q4 2024 (CyberExplorer® Datalake)	Scale known service/software users: per event, per revenue/ industry segment	Event simulation raw output (clients only)

B) Development of IED US Policy Population

The first step of building a "bottom up" IED is to determine the set of risks exposed. The insurance risks exposed to cyber catastrophic events are ultimately all businesses in the US that own a cyber policy. Thus, the base set of cyber-insured US businesses is constructed via the broad formula:

(Insured US Businesses) =
**(Count of Total US Businesses) *
(Cyber Insurance Take-up Rates)**

Count of Total US Businesses

- Sourced from the NAICS Association US Census Data as of January 2024
- US businesses classified by 6-digit NAICS codes and predefined revenue bands
- NAICS code categorizations as of 2022 (established by the U.S. Census Bureau)
  - Approximately 1,000 NAICS code categories across 9 revenue bands
  - For our analysis, we extrapolate this data into 15 revenue bands and 17 industry sectors (the "**Standard Matrix**")

Limitations of the Census Data:

- Unknown Revenue:
  - Approximately 10% of companies in the dataset have unreported revenue (vast majority are risks < $10M revenue). We manually distribute these companies across all revenue bands, in proportion to the existing revenue band % distribution.
- Broad Revenue Groupings:
  - NAICS groups all businesses with revenues between $10M and $100M into a single category, as well as all businesses with revenues over $1B.
  - To match the granularity of loss segmentation in Cyence, we subdivide the $10-100M category into three segments ($10-20M, $20-50M, $50-100M), and the $1B+ category into five segments ($1-5B, $5-10B, $10-50B, $50-100B, $100B+). Allocation of businesses into smaller bands is accomplished by plotting the curve of known ratios between Cyence universe risks and census population risks — and extrapolating more granular band counts based on that curve.
- Subsidiary counts not captured:
  - The data does not include subsidiaries. This is suitable, given that the Cyence IED reflects US loss at the parent level, so as not to double-count loss within single events.
- Exclusion of Non-Employer Businesses:
  - The dataset excludes non-employer businesses (those without employees). While these businesses are unlikely to purchase standalone cyber policies, some may still acquire bundled policies that include cyber coverage.
  - To compensate for this gap, we slightly inflate the package policy take-up rates among small businesses in our analysis

Cyber Insurance US Take-up Rates

Standalone take-up rates ascend by revenue band, while package/ endorsement rates descend (and are generally not present in mega-sized firms):

	Take-up Rates	
Revenue Band	Standalone	Package/ Endorsement
< 20M revenue (SME)	10.2%	17.8%
20M - 1B revenue (Mid)	22.9%	13.5%
1B - 10B (Large)	45.7%	9.8%
> 10B (Mega)	64.6%	0.0%

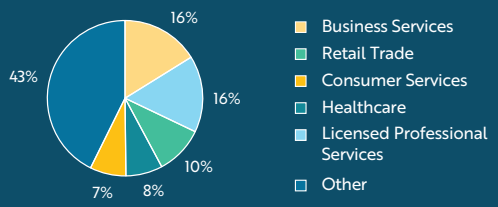
Take-up rate refers to the overall percentage of companies that purchased insurance. As a business of Marsh McLennan, GC also has access to cyber insurance rates from Marsh, another Marsh McLennan subsidiary. Cyber insurance take-up rates across all industries have been steadily increasing from about 25% in 2018 to nearly 40% in 2023. Take-up rates generally increase as revenue gets larger, ranging between 30% to 60%, depending on industry. However, it is important to note that Marsh data is potentially skewed toward larger companies, as its clientele is concentrated in large revenue bands. As such, the nearly 40% take-up rate in 2023 does not fully represent the SME segment, as shown in the take-up rate summary tables provided. Marsh has nevertheless observed growth within the SME space of monoline cyber insurance coverages, which Marsh expects to increase. Furthermore, companies in the smaller revenue bands have greater diversity and variance in take-up rates. A more refined IED may require additional granularity in SME revenue band segmentation, as more detailed data is collected in the future.

Insured US Businesses

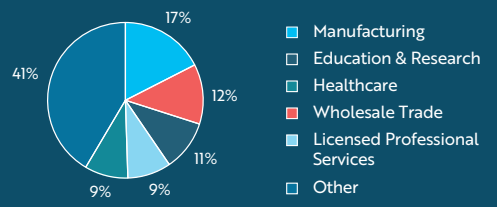
- 4.97 Million total policies
  - 98.7% SME (< 20M revenue)
  - 465 Mega sized businesses (> 10B revenue)

Top Industry Sectors

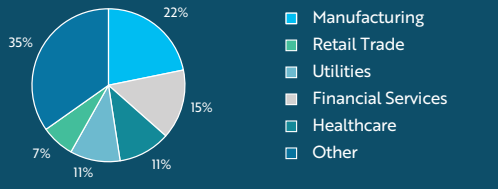
SMEs (< 20M Rev.)



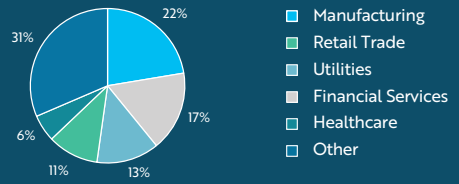
Mid (20M- 1B Rev.)



Large (1B-10B Rev.)



Mega (> 10B Rev.)



SMEs (<$20M revenue)

Business Services and Licensed Professional Services together represent nearly one-third of cyber policies in this segment. These are followed by Retail Trade, Healthcare, and Consumer Services. The remaining sectors collectively account for 43% of the total policies.

Mid-sized companies ($20M-$1B revenue)

Manufacturing is the leading sector, followed by Wholesale Trade and Education & Research. Licensed Professional Services and Healthcare also remain among the top 5 sectors in this segment.

Large and Mega companies ($1B+ revenue)

Manufacturing and Financial Services together make up nearly 40% of cyber policies in this group. Healthcare remains a key contributor within the top 5 sectors, alongside Utilities and Retail Trade. Other sectors comprise about one-third of the total policies for this revenue tier.

- Every business is assigned a primary policy, and excess policies are distributed among a percentage of larger risks.
- US census data implies a US business count of approximately 17 million, where we estimate 28% of these businesses to be insured for cyber. The take-up rates for Micro businesses (< $500k revenue) is substantially lower than that of a $20M+ revenue business.
  - A 28% take-up for SMEs is a higher estimate than seen in recent publications and industry conferences. We attribute this to the removal of all subsidiary companies, in addition to the exclusion of non-employer businesses from the base population count.
- The displayed industry sectors represent the most widely insured segments of the population. Business, Consumer and Licensed Professional Services comprise a majority of the SME space; they are often made up of single incorporated individuals or very small/role-specific services.
- In this exercise, we address Package and Endorsement policies by removing different coverage categories at observed rates in the cyber policy market, with randomized dispersion across the 3.1 million policy set. Removing coverages materially impacts potential frequency and severity of claims.

	US Businesses		US Policies		Take-up Rates
Industry Demographics	**17,714,924**		**4,970,956**	**(Primary)**	**28.1%**
< 20M revenue (SME)	17,545,830	99.0%	4,908,278	98.7%	28.0%
20M - 1B revenue (Mid)	162,964	0.9%	59,215	1.2%	36.3%
1B - 10B (Large)	5,411	0.0%	2,998	0.1%	55.4%
> 10B (Mega)	720	0.0%	465	0.0%	64.6%
Standalone			1,821,167	36.6%	
Package / Endorsement			3,149,789	63.4%	
Primary			4,970,956	100.0%	
Excess*			5,388	0.1%	
Business Services			813,089	16.4%	
Licensed Professional Services			801,127	16.1%	
Retail Trade			508,368	10.2%	
Healthcare			385,973	7.8%	
Consumer Services			376,871	7.6%	
All Other			2,085,527	42.0%	

*Approximate count of full excess towers in market: individual layers collapsed into towers, limits summed and min attachment point referenced

C) GC Average Policy Terms

Average Policy Terms by Revenue Band ($ thousands):

	Average Premium			Average Limit		
Revenue Band	Standalone	Package/ Endorsement	Excess*	Standalone	Package/ Endorsement	Excess*
< 20M revenue (SME)	1.7	0.7	2.3	1281.8	146.3	7992.3
20M - 1B revenue (Mid)	34.9	7.2	24.9	2293.6	204.5	10477.3
1B - 10B revenue (Large)	225.4	39.3	267.5	6472.9	269.2	23872.7
> 10B revenue (Mega)	813.9	-	2277.6	12795.0	-	132643.7

	Average Per Occurrence Retention			Average Attachment		
Revenue Band	Standalone	Package/ Endorsement	Excess*	Standalone	Package/ Endorsement	Excess*
< 20M revenue (SME)	3.5	1.4	10.3			1607.6
20M - 1B revenue (Mid)	75.3	14.8	201.7			3355.0
1B - 10B revenue (Large)	4306.6	152.1	4308.6			6473.8
> 10B revenue (Mega)	28340.4	-	28340.4			12796.0

* Excess premium and limit summed across tower; excess attachment the average minimum of the tower

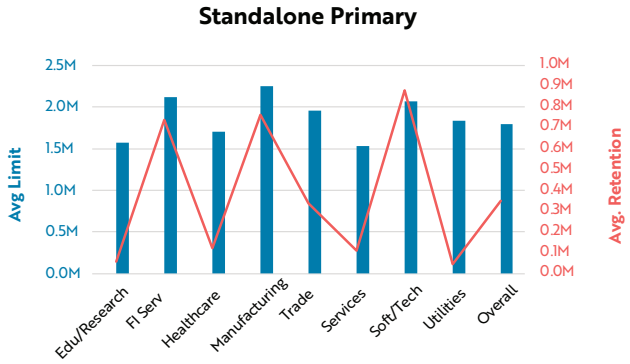
Policy Term Relativities by Sector

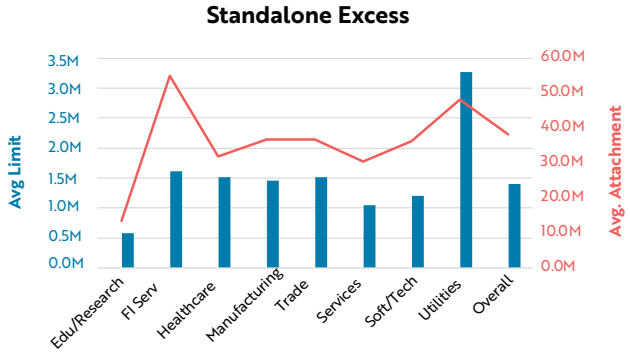
GC's CyberExplorer® Datalake is a robust database of actual client claims information, exposure details and policy terms, vendor model output and actual treaty statistics from cyber reinsurance transactions. It encompasses a diverse mix of cyber portfolios from different company sizes, industry concentrations and geographic jurisdictions. Using the latest 2024 data available at the time of analysis, average policy terms — including retentions, attachment points, limits and premium — were pulled. The data was broken out by cyber standalone versus package/endorsement policies, primary versus excess coverage, industry sector and granular revenue band.

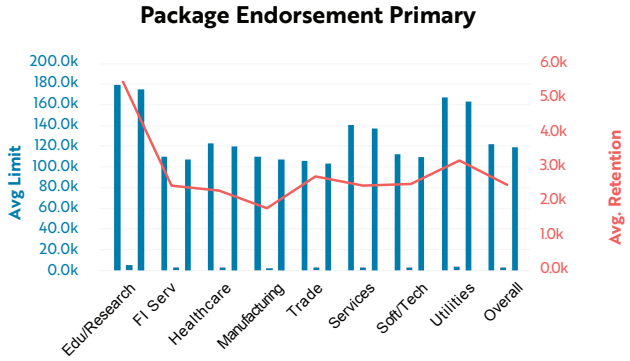
The charts provided show average policy terms by industry for standalone primary, standalone excess, and package/endorsement primary policies in terms of attachment points and the limits.

- Excess policies on average attach between $30-40M and have limits between $10-20M. Note, however, that the stats provided are in total across excess programs: premiums and limits are summed up across the tower, and attachment points apply to the lowest layer on a given program.
- Standalone primary policies have a wide range of retentions but are typically under $1M and average limits between $1-2M.
- Package and endorsement policies generally have significantly lower terms than their standalone counterparts, with retentions in the $2,000-$3,000 range and limits between $100k and $200k.

While GC has deep market penetration, the firm does not represent all cyber insurers in the industry. The policy information collected by GC is from individual cyber portfolios' reinsurance submissions, rather than the full insurance tower on an individual-insured basis, which means the data may be missing some layers in a multi-layer program. However, given GC's market share in the affirmative cyber reinsurance treaty business, we do not anticipate this to lead to material bias in the exposure assumptions.







D) Cyence Model 7 Baseline Population Universe

In order to project losses across the entire US insured market, Cyence begins with a smaller subset of US risks, which are known (the Cyence Baseline Population), and then scales known risk results to US population level. Cyence currently holds firmographic and technographic detail on a population of approximately 600,000 US businesses and subsidiaries. This set has been further refined to 200,000 for the purposes of this exercise, to isolate uniquely recognized parent-level organizations specifically and remove any possible duplicated loss from subsidiary additions. This aligns Cyence loss generation with the parent-only exposure collection. The breakout of these firms across revenue bands is shown below, by count and projected loss, to give a sense of what the Cyence M7 US universe coverage looks like as the starting point:

	Counts			Expected Loss ($M)		
Revenue Band	**Cyence Universe**	**Full US Insured Risks**	**Cyence Universe Base %**	**Cyence Universe**	**US Insured Risks**	**Cyence Universe Base %**
< 20M revenue (SME)	152,217	4,908,278	3%	127.3M	2487.1M	5%
20M - 1B revenue (Mid)	39,515	59,215	67%	559.8M	799.5M	70%
1B - 10B (Large)	2,212	2,998	74%	587.7M	761.7M	77%
> 10B (Mega)	416	465	89%	898.3M	998.3M	90%
Total	**194,360**	**4,970,956**	**4%**	**2173.1M**	**5046.6M**	**43%**
Sector	**Cyence Universe**	**Full US Insured Risks**	**Cyence Universe Base %**	**Cyence Universe**	**US Insured Risks**	**Cyence Universe Base %**
Business Services	28,153	808,681	3%	140.0M	527.4M	27%
Retail Trade	14,482	508,213	3%	126.7M	267.7M	47%
Licensed Professional Services	30,240	799,100	4%	63.0M	427.0M	15%
Healthcare	14,713	386,775	4%	143.0M	369.0M	39%
Manufacturing	18,085	190,997	9%	437.8M	654.1M	67%
Financial Services	18,175	352,843	5%	323.6M	631.7M	51%
Education & Research	11,265	173,607	6%	222.3M	356.1M	62%
Wholesale Trade	13,390	193,234	7%	47.2M	134.3M	35%
Other	45,857	1,557,506	3%	669.4M	1679.2M	40%
Total	**194,360**	**4,970,956**	**4%**	**2173.1M**	**5046.6M**	**43%**

Note that the Cyence base universe only holds approximately 4% of total estimated cyber policy counts in the US, but represents 43% of total expected US gross loss.

E) Testing: Written Premium, Loss Ratio, Ground-Up vs. Gross Loss

Revenue Band	Total US Policies*	Average Written Premium Per Policy			EST. US WRITTEN PREMIUM ($M)
		Standalone	Package	Excess	
< 20M revenue (SME)	4,908,584	$1,696	$747	$2,324	**$5357.4M**
20M - 1B revenue (Mid)	61,374	$34,796	$7,153	$25,015	**$1507.4M**
1B - 10B (Large)	5,456	$225,277	$39,277	$267,400	**$1234.5M**
> 10B (Mega)	930	$806,691		$2,245,423	**$1419.2M**
Total	**4,976,344**				**$9518.6M**

Revenue Band	Cyence Modelled Expected Loss		Insurance Coverage Ratio	EST. US GROSS LOSS RATIO
	GROUND-UP **	GROSS		
< 20M revenue (SME)	**$5044.8M**	**$2487.1M**	49%	**46.4%**
20M - 1B revenue (Mid)	**$2000.8M**	**$799.5M**	40%	**53.0%**
1B - 10B (Large)	**$2534.1M**	**$761.7M**	30%	**61.7%**
> 10B (Mega)	**$3734.2M**	**$998.3M**	27%	**70.3%**
Total	**$13313.8M**	**$5046.6M**	38%	**53.0%**

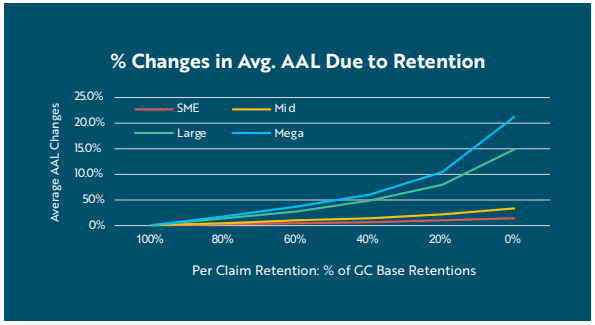
*** Excess counts represent full towers in market**
**** Ground-up loss estimate only for US businesses with a cyber policy**

Total estimated written premium of $9.52B represents the US cyber market as of hypothetical Policy/Calendar year 2024. The figure is roughly in line with the low-end of the range provided in the GC publication **Behind the Firewall: 2024 Global Cyber Industry Insights** ($10.2B - $10.8B). Note that the 5% difference arises due to mutually independent estimates being made at different points in the year, and via different methods.

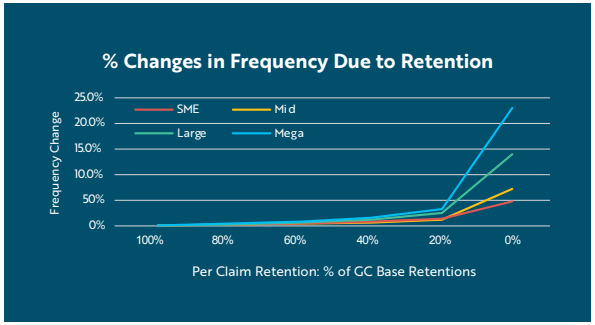
Regarding the 53% expected industry loss ratio: based on data from GC, the highest annual cyber loss ratios on a historical basis occurred in 2019 and 2020, with ratios in the low- to mid-70s. More disciplined underwriting after these ransomware-impacted years yielded a much more stable industry performance between 2022 through 2024, with 2022 being the lowest point in the mid-30s, due to the lack of ransomware activity. Despite recent signs of loss ratio deterioration, due to softening rate environment and occurrence of cat-like cyber events, such as the CDK attack and the CrowdStrike incident, the mid-50s modeled expected loss ratio is broadly in line with the industry's historical performance, adjusted to be on a go-forward basis.

Insurance loss coverage ratios (gross to ground-up loss) decrease as company size increases. Larger enterprises typically choose higher retentions and self-insure lower severity risks, while maintaining insurance primarily for catastrophic scenarios. This means larger organizations have a smaller portion of their total ground-up losses covered by insurance, as high volumes of smaller, more trivial events are retained. In the tables below, if we assume that the IED baseline retentions represent the "100% Basis" (far left column), we can test the % change impacts on insured frequency and insured average annual loss (AAL) as we reduce retention levels in 20% increments:

% Changes in Avg. AAL Due to Retention						
Avg. AAL Change	Per Claim Retention: % of GC Provided Retentions					
Rev. Band	**100%**	**80%**	**60%**	**40%**	**20%**	**0%**
SME	0%	2%	4%	6%	8%	13%
Mid	0%	4%	8%	14%	21%	32%
Large	0%	12%	27%	47%	79%	147%
Mega	0%	16%	35%	60%	103%	211%



% Changes in Frequency Due to Retention						
Frequency Change	Per Claim Retention: % of GC Provided Retentions					
Rev. Band	**100%**	**80%**	**60%**	**40%**	**20%**	**0%**
SME	0%	9%	21%	44%	95%	570%
Mid	0%	12%	28%	54%	101%	370%
Large	0%	19%	48%	93%	187%	1111%
Mega	0%	25%	62%	121%	260%	1840%



A reduction in insurance retention levels disproportionately increases claim frequency over AAL because it brings a multitude of smaller, previously self-insured cyber events above the claiming threshold. Due generally to the heavy-tailed severity of cyber losses, high volumes of minor claims still contribute relatively less to AAL than do the larger, less-frequent events.

Concurrently, lowering retentions impacts AAL more significantly for large businesses than it does for SMEs. Large enterprises typically hold higher average retentions to begin with, based on the ability for large enterprises to absorb small losses internally. Along with this, large enterprises are exposed to far more severe loss events generally, between breaches of many millions of records and associated lawsuits, as well as exponentially higher potential BI costs per unit time of interruption. Therefore, a 20% incremental reduction in retention has a more substantial impact on large businesses within these extremely severe events.

F) Cyence Model 7 IED Tail Event Sets

Regarding potential cyber cat events, the Cyence model projects the following 11 accumulation paths to populate the OEP curve tail beyond the 1-in-50 year return period:

IED Tail Event	Malicious/Non	Commentary
Hypervisor Outage	Malicious	Xen, MS Hyper-V, VMware, Oracle VM: shared VM compromised via hypervisor software
Hypervisor Outage	Non-Malicious	Bad hypervisor software update
AWS US Cloud Outage	Malicious	Est. 2.2M AWS users in US (Largest market share)
AWS US Cloud Outage	Non-Malicious	
Azure US Cloud Outage	Malicious	85% of Fortune 500 companies use Azure
Azure US Cloud Outage	Non-Malicious	
Windows OS Mass Data Breach	Malicious	Zero-day exploit via software vulnerability; bot-driven data exfiltration deployed across many firms simultaneously
Windows OS Mass RW Deployment	Malicious	Mass deployment of ransom malware vis OS vulnerability; BI, forensics and ransom related costs
Apache Http Server Mass RW Deployment	Malicious	Apache: Open source software used for web hosting specifically; often runs on Windows or Linux OS
Linux OS Mass RW Deployment	Malicious	Linux OS: 4% market share; but high concentration in server environments/ supercomputing space
Nginx OS Mass RW Deployment	Malicious	NGINX: Open source web server, with focus on caching and performance enhancement

Points to note on the event set

- The events above are part of the Cyence Model 7 stochastic event set, among thousands of other potential accumulation vectors. These 11 paths, however, comprise the entirety of the Cyence OEP (largest event per sim year) beyond the 1-in-50 return period. The 1-in-50 threshold was selected because the number of tail-contributing cat event paths increases quickly below 1-in-50. The project requires individual aggregation path market share research to project to the full US population, and 11 paths in the tail were a manageable research task.
- The IED event set focuses exclusively on digital attack vectors and digitally-based supply-chain disruption, while physical attack vectors and physical supply-chain repercussions remain outside the scope of this project.
  - It is worth noting that the majority of cyber insurance policies do not cover physical supply-chain events, based on how dependent business interruption or contingent business interruption are defined in policy language.
  - While there are a few cyber policies in the market that do cover direct physical suppliers (assuming there is a direct contract between the supplier and the insured, and the cyber event at the supplier qualifies as a covered cyber event under the policy), these remain a minority. Policies that extend coverage to physical supply-chain impacts are not widely available in the current cyber insurance market.
- The set above includes "Nation-State Attributable" events, with no further modeling assumption on their potential insurability.

G) Reflecting Cyence Universe Cat Tail Across US Population

The Cyence universe baseline population consists of approximately 200,000 cyber policies. Within the Cyence accumulation model, many of these policies share common exposures to cat accumulation paths. Based on these in-house per-company network/provider reliance observations, along with market research on total US businesses exposed to each cat exposure (listed in Section F), Cyence uses a controlled scaling method to extrapolate US-insured population cat events. Scaling is uniquely applied per event, per revenue band and per sector to reflect individual characteristics of each event type and affected population. See the table below for a calculation example for a Linux OS event in the IED tail, for a specific revenue band/sector:

This process is repeated for each of the 200 IED OEP events individually, for each of 15 * 17 = 255 revenue / sector buckets, and across policy types (Standard, Package / Endorsement, Excess).

Note: This method makes the broad assumption that software usage rates at Standard Matrix granularity are constant between the Cyence universe and larger population. We recognize the potential for bias within this assumption. However, usage bias is mitigated in the following ways:

- The vast majority of large risks are known to Cyence and included in the base set ($20M+ revenue, see Section D), representing approximately 50% of projected US-insured loss).
- For SMEs, the base Cyence population includes 152,000 identified risks. This is of course a fraction of insured risks across the entire US, but still a substantial and material subset from which to infer credible service usage ratios.

	Counts of Businesses for Scaling		
	Cyence Population	US Population	Note
Total	200k	17.7M	
+ with Cyber policy	**200k**	4.97M	**- Businesses captured in Cyence Pop.**
+ in $50-100M Rev. band (B)	5.3k	13.3k	**all assumed to have a policy**
+ in FI Services sector (S)	300	1.2k	
+ users of Linux OS (P)	94	488	
+ impacted by Linux OS Event (X)	10	**52**	**= (10) * (488) / (94)**
Gross Loss $ Event (X): Rev. Band (B), Sector (S), Event Path (P)	$180k	**$936k**	**= (180) * (52) / (10)**

Required AEP Scaling Calculations

Attritional Events

The scaling process for attritional losses follows purely from population relativities, between the base Cyence population and the projected US population (by Standard Matrix granularity):

- **(US Pop. Attritional Loss) =** (US Pop. Risk Count) / (Cyence Pop. Risk Count) * (Cyence Pop. Gross Loss)

Other Accumulation Events

For accumulation events not part of the 11 predefined events representing the extreme tail, appropriate expected loss scaling factors are estimated using the 11 predefined paths as proxies. Specifically, the ratio of (U.S. gross loss) : (Cyence gross loss) derived from the work on extreme tail events is then applied as scalar for all other cat accumulation events in the Cyence event set, on an expected loss basis only. Cyence would argue that this can be a conservative modeling assumption in the AAL to a small degree, given that the largest aggregation paths in the analysis generally have far more users than other paths. Nevertheless, Cyence does not expect the other cat accumulation events would penetrate the extreme tail EP curve materially beyond the 1-in-50, even if individually scaled.

Cyence Model 8 and Future Iterations of IED

The current Cyence Model 7 IED results here are only the first iteration of a much larger project, as Cyence and GC plan to perpetuate and evolve the IED product over future model versions. Cyence Model 8 will be released in phases over 2026, and will feature a more technographic-driven basis for industry exposure, among other features:

- Full mapping of world industries via domain identification (more than 250 million domains available for distribution across all countries)
- Added event sets (SaaS/PaaS SPOFs, Mass Non-Malicious Software Update, Business Email Compromise)
- Global IED, with geo-granularity and aggregation capability
- Enhanced ability to supplement portfolios with minimal to no per-risk detail available, with sensitivity analysis surrounding unknown risks
- IED tracking: Industry influences that impact the shape of IED tail curve over time (rate swings, market growth, population shifts and average adjustments to policy terms)
- "Top Down" market share approach: Additional ability to estimate exposure to cat loss based on known percentages of market written premium
- Marginal Impact tool, for projected portfolio expansion into new market segments

Closing Remarks

Thank you for your time and attention to this document and its detail. We acknowledge the uncertainty surrounding a scaling exercise of this magnitude in the SME space, but we are confident that our extensive US market-share research across all tail contributing event paths can provide a reasonable and realistic collection of industry loss scenarios.

The Cyence IED/ILC event set is fundamentally data-driven in all parameter selections; there are no elements of event narrative present that have not been observed in history in some shape or form. Thus, the uncertainty in the extreme tail presented is purely a question of magnitude, not of technical possibility.

The GC exposure set is both extensive and credible at a detailed level of granularity. With this volume and quality of exposure data, the IED/ILC project will be able to track detailed market shifts and corresponding shifts to the EP curve as we move into the future with this exercise. Once again, we hope to gain the trust and the collaboration of the cyber market at large with the transparency of method we have provided in this document, and we will continue to provide a consistent source of cyber industry loss exposure moving forward across all future model releases.

Cyence and GC encourage any and all feedback regarding the IED / ILC construction process outlined here, and we look forward to the discussion.

Contributors

Brian Choi, Lead Data Scientist
Guidewire Cyence

Brian recently rejoined the Modeling and Data Science team at Guidewire-Cyence, focusing on updates related to our attritional models and the use of these models for live inference applications in the underwriting process. Before joining Guidewire, Brian worked as an actuary and data scientist at Liberty Mutual Insurance and two insurance startups. Brian is a holder of several insurance certifications, including Fellow of the Casualty Actuarial Society (FCAS), Chartered Property and Casualty Underwriter (CPCU), and Associate in Reinsurance (ARe). He earned his BA in Biochemistry and an MS in Actuarial Science from Columbia University, New York.

Jess Fung, Managing Director – NA Cyber Analytics Lead
Guy Carpenter

Jess is GC's North America Cyber Analytics Lead. She oversees cyber catastrophe and actuarial modeling, advisory services, proprietary data lake creation, and thought leadership research to support GC's North American and Global clients. She also serves as the Head of Analytics Sales – North America, spearheading various strategic initiatives to deliver consistent, best-in-class analytics content and insights in RFPs and new business pursuits. Jess has a Bachelor's Degree with High Distinction in Applied Mathematics from the University of California, Berkeley. She is a Fellow of the Casualty Actuarial Society and a Member of the American Academy of Actuaries.

Maurizio Gobbato, Head of Cyber Catastrophe Modeling
Guidewire Cyence

Maurizio joined Guidewire in 2022. He leads the Modeling team and is responsible for the development, calibration, and validation of the cyber risk models. Before joining Guidewire, he was a Senior Catastrophe Modeling Analyst at USAA, where he led the onboarding and business implementation of third-party vendor models. Prior to USAA, Maurizio was a Principal Modeler for the Model Development team at Risk Management Solutions (RMS), where he led the development and updating of their earthquake, terrorism, and workers' compensation models. Maurizio holds a PhD and an MS in Structural Engineering from the University of California, San Diego, and a BS in Civil Engineering from the University of Padova, Italy.

Shu Iida, Senior Vice President – Cyber Catastrophe Analytics
Guy Carpenter

Shu joined the GC Cyber Center of Excellence as a senior cat modeler in November 2020. He is responsible for leading the cyber catastrophe modeling team and developing proprietary tools to provide insights to clients. He also works closely with cyber model vendors to build their products and share this knowledge with clients and prospects. Shu graduated from the University of California, Berkeley, with a Bachelor's Degree in Civil and Environmental Engineering. He holds a professional designation as an Associate in Reinsurance (ARe).

Douglas Stromberg, Director of Product Management
Guidewire Cyence

Douglas is the primary actuarial and business representative for Cyence. He is a primary director of product direction and overseer/creator of model content. He also supports the Cyence model development team and is the main contact for Cyence reinsurance modeling. Douglas' most recent experience before Guidewire was in stochastic modeling and reinsurance structuring for a prominent market brokerage over eight years. Douglas earned his MS in Applied Mathematics from DePaul University Chicago, and is an Associate in the Casualty Actuarial Society.

Ariel Yeung, Principal Data Scientist
Guidewire Cyence

Ariel joined Guidewire in 2019 and has experience working on attritional and accumulation models, including the targeted data breach, ransomware, and service provider models. Before joining Guidewire, Ariel worked on pricing insurance policies at Progressive Insurance. She holds an MS in Business Analytics from Santa Clara University and a BS in Statistics from the University of California, Los Angeles.