Gallagher Re

A History of Near Misses

Utilizing counterfactual analysis to understand cyber risk

In association with

CyberCube

Key Takeaways

- Counterfactual analysis can show how cyber attacks may have been quantifiably worse if circumstances had evolved differently.
- They are especially useful in the cyber insurance market, whose short historical catalogue contains only a few notable events. Moreover, due to the dynamic nature of this risk, no two events are ever the same — so counterfactuals can help explore alternative event characteristics, narratives, and losses.
- Gallagher Re has worked with CyberCube on several example counterfactuals, which can produce significant variation in losses. Plausible changes to event characteristics can increase insured industry losses from tens or hundreds of millions, to multiple billions.
- Cyber carriers can use counterfactual analyses to deepen their understanding of cyber threats, improve their cyber models, stress test their portfolios, and produce a more fully-evidenced view of risk.
- The ability to analyze historical events in the context of current technological and threat conditions will be a vital tool for insurers in differentiating themselves from their peers, and maintaining or gaining vital underwriting capacity.

Introduction

For any carrier wanting to grow and access new capacity it is critical that they can rigorously assess and communicate the risk in their portfolios, but new cyber carriers face a particular challenge: a lack of good data on past losses.

Traditional risk management practices are heavily dependent on using past events to understand future potential outcomes. But there is only a short history of meaningful cyber losses, stretching no further back than the 1990s. The catalogue contains many events unlikely to be repeated, and a few extreme catastrophic scenarios. So backwards-looking statistical methods are not always appropriate.

Insurers need to explore alternative approaches. Counterfactual analysis is an underutilized tool that presents an opportunity for cyber modeling, as it can be used to develop a deeper understanding of past events and the severity of potential extreme losses in the future.

This paper explores the benefits of counterfactual analysis for cyber (re)insurers and provides a framework that can help exposure risk managers, actuaries, and catastrophe modelers incorporate it into their standard suite of risk assessment tools. The paper also contains some worked examples of cyber counterfactual analysis that Gallagher Re has conducted in collaboration with CyberCube.

What is Counterfactual Analysis?

Counterfactual analysis is the process of reimagining a historic event by changing some of its key characteristics and quantifying the resulting impact on the losses. In the insurance industry it is common for companies, following a year of adverse losses, to retrospectively assess how large events could have been avoided or lessened.

However, in years of profitable underwriting there is often little incentive to consider how recent events could have been worse. This is known as a downward counterfactual. Cyber's lack of a sufficiently large and complete catalogue of historic loss events makes counterfactual analysis particularly useful.

Benefits of Counterfactual Analysis

The primary gain from completing cyber counterfactuals is being able to generate scenarios that can be used to stress test an insurer's portfolio. It can assist with validating the tail of model outputs or risk understanding, and can ensure that these scenarios remain plausible and realistic.

Key Benefits of Downward Counterfactual Analysis

- Explores tail risk
- Extends the severity range of historic events in a plausible way
- Facilitates deeper understanding of cyber risk
- Back-tests model results
- Mitigates bias in model calibration
- Provides systematic approach to creating Realistic Disaster Scenarios (RDSs)
- Expands claims books and loss catalogues

A cyber event is not a singular incident that happens in an instant, such as an earthquake; it is a complex timeline of threat actor decisions, defensive cybersecurity actions, aggravating external influences, and random chance. Therefore, each historical cyber event is just one realization of a multitude of potential outcomes, and it is highly plausible that an inconsequential historic event was actually a near-miss, which had the potential to cause an extreme cyber loss if things had transpired differently. Performing a counterfactual analysis enables insurers to expand the severity range of their historic catalogues, providing more extreme events with which to assess the cyber exposure in their portfolios.

An alternative approach could be to create risk scenarios from first principles, but this has drawbacks. Using historical events to conduct these exposure and risk investigations gives more weight to the outcome, because any reimagined event narrative will have its basis in the real world. This can ease the communication of cyber risk to less knowledgeable or more sceptical decision-makers and risk officers within a company.

Those conducting a downward counterfactual analysis exercise also benefit from deepening their understanding of how cyber attacks occur and develop. Identifying and studying the most effective defensive decisions and beneficial cybersecurity practices can inform underwriting processes and allow for bad risks to be avoided.

Downward counterfactual risk analysis also strengthens model validation. Cyber model vendors mostly rely on the same historic datasets and market feedback to build and calibrate their models, and these same datasets and market views are typically all that cyber catastrophe analysts have available to test the models with. This predicament obviously introduces a level of bias into any validation efforts, but this can be reduced by generating a counterfactual alternative dataset with which to test the models.

The Elements of a Cyber Attack

In our initial analyses of historical cyber events, Gallagher Re has observed recurring factors that were often the primary drivers of the severity of losses. These factors can be grouped under several broad headings — some are characteristics of the firm targeted; some capture the spread of the impact; and others are mitigating techniques such as the presence of cybersecurity controls.

We have categorized these factors into sixteen key elements of a cyber event:

Event Criteria	Element	Guidance
Target	Firmographic	Consideration of how the targeted company or industry sector impacted the trajectory and subsequent impact of the event.
	Footprint	Developing an understanding of how many insured companies were affected and what percentage of the insurer's cyber portfolio suffered losses.
Environmental	Jurisdiction	Consideration of how the nature of the incident would change in a different geographic/ regulatory environment.
	Timeframe	Analyzing how the timeframe of exploitation was a driver of the loss outcome.
	Regulatory	Identifying relevant legislation and industry regulation and how this could increase or decrease the financial impact of the attack.
	Exclusions	Applying relevant exclusionary language to the event.
	Political	Understanding how the political landscape at the time influenced the attack.
	Vulnerabilities	Consideration of how known (widespread) and unknown vulnerabilities were utilized to conduct the attack.
Impact	Propagation	Analyzing how the nature and spread of any malware present in the attack changed the overall severity of the event.
	Impact Scaling	Identifying new elements that could be introduced to the attack to make the outcome worse than the original event.
	Business Impact	Consideration of business downtime and reputation.
	Records	Investigating how the number/percentage of records impacted by the attack could alter the overall severity.
	Ransom Payment	Looking at whether a ransom was paid upon demand and how that decision was made.
Cybersecurity	Security Controls	Investigating how a company's security controls influenced the severity of the attack.
	Detection	Identifying whether detection mechanisms altered the severity of the event.
	Response and Recovery	Consideration of if and how a company's response and recovery approach changed the trajectory of business impact.

There may only be a few elements that are significant drivers of any one event, but it is important to consider them all during the initial stages of a counterfactual analysis. There is no single element that is consistently material and relevant for each event or attack type.

Cyber Downward Counterfactual Process

To conduct our counterfactual analyses, Gallagher Re incorporated the concept of cyber counterfactual elements into the six-step guiding framework that was laid out by Lin et al. (2020):[1]

1. **Event Identification:** Identify events that have had a significant impact, either economically or in terms of insurance claims (for example, we considered the 2022 Rackspace outage event). Collect information about the event timeline and reported elements. Categorize events into specific perils, such as malware or service provider outages.

2. **Element Analysis:** Using Gallagher Re's counterfactual framework, determine the elements (sometimes referred to as parameters) of each identified event. Where the parameter proves to have limited relevance or impact, remove it from deeper analysis.

3. **Element Adjustment Range:** For those elements which prove to have a significant effect on the trajectory of the event, define the maximum magnitude of adjustments to determine how they can be varied within the realm of plausibility. Consideration should be made to the co-dependencies between some parameters. For example, switching the "target industry" sector is likely to affect the "decision to pay ransom".

4. **Apply Element Changes:** To create a version of the event with greater impact.

5. **Quantitative Output:** Conduct a numerical analysis based upon the changes made to the key event parameters in order to determine the difference (or 'delta') between actual losses and counterfactual losses.

6. **Counterfactual Event Definitions:** Utilizing the information generated from previous steps, produce a final scenario narrative and losses.

[1]Lin, Yolanda C., et al. "Modeling Downward Counterfactual Events: Unrealized Disasters and Why They Matter, *Frontiers in Earth Science*, vol. 8, 06 November 2020.

Case Studies

The following case studies are the outcomes of a collaboration between Gallagher Re and CyberCube. The event selection, initial analysis, and process were provided by Gallagher Re, while the counterfactual narratives and loss quantification were generated by CyberCube.

These case studies are intended to show that a cyber counterfactual analysis does not need to be highly technical for a notable impact on the event outcome to be realized, and therefore counterfactual analysis can be a highly accessible and easily deliverable undertaking.

The actual (historical) scenario is presented as the baseline for each study, with each subsequent change being a compounding impact on the loss. Each event was simulated using the counterfactual parameters to generate a distribution of potential loss outcomes.

Case Study: Kaseya

Event Selection

As an indiscriminate supply chain attack, the 2021 attack on US software provider Kaseya brings into focus the impact of malicious cyber activity against Managed Service Providers (MSPs). A deep dive into the parameters of this event, exploring how the impact could have been different, helps insurers understand and prepare for an anticipated increase in such sophisticated supply chain attacks.

Event Narrative: Baseline

In July 2021, Kaseya discovered its products had been used to infect roughly 1,500 organizations around the world.

The attack targeted Kaseya's Virtual System Administrator (VSA) software, a tool used by Managed Service Providers (MSPs) to manage and monitor the IT infrastructure of their customers. By exploiting zero-day vulnerabilities in Kaseya's software, attackers were able to distribute ransomware through it (known as a supply chain injection attack), affecting not just the MSPs but also their customers. The ransomware was delivered to all on-site servers in the form of a fake management update.

The ransomware, believed to be from the REvil group, encrypted files on the affected systems, rendering them inaccessible. REvil demanded a ransom of over USD50 million in exchange for the decryption key.

On July 22, Kaseya announced that it had obtained a decryption tool from an undisclosed 'third party' and was working to restore the impacted environments. The lack of transparency led to speculation that Kaseya had paid the ransom.

Event Narrative: Counterfactual Changes

For Kaseya, three 'Impact' elements were considered to have the greatest counterfactual relevance. Although additional elements were identified as having counterfactual potential, Gallagher Re and CyberCube wanted to keep the case studies in this paper succinct and accessible.

These counterfactual steps compound, meaning each successive step builds upon the last, slowly adapting the narrative details.

Counterfactual 1: SaaS Compromise

Criteria	Element	Counterfactual Changes
Impact	Propagation	SaaS Compromise Consider the effect of a wider distribution of the malicious update beyond Kaseya's VSA clients, to clients of its Software as a Service (SaaS) proposition. This would have impacted a larger client base, resulting in widespread disruption and an inability to access data.

Kaseya stated that its IT Complete suite of products was 'minimally affected by the breach' with only one (that being VSA) out of 'its 27 modules' compromised. A wider infection could have infected many more of the roughly '800,000 to 1,000,000 local and small businesses' that are managed by Kaseya's customers (MSPs).

Counterfactual 2: Insufficient Incident Response

Criteria	Element	Counterfactual Changes
Impact	Business Impact	Insufficient Incident Response Consider a greater downstream deployment rate of ransomware through the wider Software as a Service (SaaS) client base.

This assumes that Kaseya was slow to implement its remediation and mitigation measures, leading to a **longer dwell time, or 'saturation period', before ransomware deployment** and a larger proportion of the client base installing the malicious software update. This would make more clients prone to infection before the payload was deployed. The attack would have a more extensive impact, with approximately 1/3 of Kaseya's 35,000 customers being breached.

Counterfactual 3: Wiperware

Criteria	Element	Counterfactual Changes
Impact	Impact Scaling	Wiperware Consider the deployment of wiper malware instead of ransomware. Payload appears to be ransomware, but in reality the encryption bricks/wipes data and sabotages hardware components while demanding a ransom.

Wiper malware would have made recovery efforts far more difficult and costly. Companies may not have had a choice but to pay a ransom to restore services only to find unbootable systems with corrupted or wiped firmware. This type of attack would render hardware inoperable, and can often spread much faster than traditional ransomware as total damage is the focus.

If wiper malware were deployed after a larger infection against more of Kaseya's services and client base, the outcome could have been a much wider and more destructive event.

Counterfactual Loss Quantification

Table 1: CyberCube's counterfactual parameters and losses for Kaseya

		Kaseya			
Criteria	**Counterfactual Analysis**	**Baseline**	**Higher Infection Rate**	**Deployment Downstream**	**Wiperware**
Footprint	**Direct Customers (MSP Companies)**	35,000	35,000	35,000	35,000
	Claimed Infection Systems	1,000,000	2,000,000	2,000,000	2,000,000
	Downstream Infection Rate	10%	20%	20%	20%
	Infected Companies	100,000	200,000	200,000	200,000
	Dwell time	10%	20%	20%	20%
	Downstream Deployment Rate	15%	15%	30%	30%
	Downstream Infected Customers	1,500	6,000	12,000	12,000
	SPoF Control Failure	39%	49%	49%	49%
	Impact Rate	31%	31%	31%	62%
	# Impacted Companies	181	911	1,823	3,646
Severity	Payload	Ransomware	Ransomware	Ransomware	Wiperware
	Financial Claims Rate	39%	44%	46%	49%
	# Companies filing claims	70	399	845	1,786
	$M insured loss (conditional distribution)				
	5th	$12	$209	$586	$2,323
	50th	$58	$451	$968	$3,100
	95th	$230	$801	$1,538	$4,032

- Green and Blue rows represent commonly reported or known figures that tie the real world events to modelled events
- Green text represents known reported figures for these events (i.e. "baseline")
- Blue text represents changes in figures (model parameters) as each counterfactual step is added

kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/
https://www.theverge.com/2021/7/5/22564054/ransomware-revil-kaseya-coop
https://www.crn.com/news/security/kaseya-vsa-saas-coming-back-tuesday-on-prem-wednesday
https://www.crn.com/slide-shows/security/huntress-ceo-kyle-hanslovan-to-msps-on-kaseya-ransomware-attack-get-it-together-or-go-out-of-business
https://therecord.media/kaseya-more-than-1500-downstream-businesses-impacted-by-ransomware-attack
https://www.csoonline.com/article/571081/the-kaseya-ransomware-attack-a-timeline.html

Understanding the Footprint

- SPoF Control Failure: This considers the percentage of systems where SPoF control failure over the course of the attack leads to impacted end users. Examples are unapplied patches, lack of malware detection, or lack of security control effectiveness. Increases would represent more systems where SPoF controls failed.
- Downstream Infection Rate: Details the ratio of the claimed total infected systems at end users (as claimed by threat actors) to the known total Kaseya customers (like MSPs). Conversion from companies to total computers was performed using CyberCube datasets. Increases would mean a greater reported spread of infection to systems.
- Downstream Deployment Rate: Explores the conversion rate from infection calculation to reported systems where deployment impacted end users (successful payload deployment). Increases would mean a greater reported rate of successful payload deployment to customers (not just infection).
- Financial Claims Rate: The percentage of companies with both Insurance and an impact to the degree that they need to file a claim.

Case Study: Rackspace

Event Selection

The 2022 attack on cloud services provider Rackspace is an excellent candidate for counterfactual study because the event could easily have resulted in catastrophic losses. Rackspace is a key player in the market for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) hosting providers. Yet, the quick migration of customers to Microsoft 365 proved that redundancy options have the power to completely shift the trajectory of a catastrophic cyber event.

Event Narrative: Baseline

In December 2022, Rackspace experienced a ransomware attack that affected its hosted Microsoft Exchange environment. Rackspace later confirmed that Play Ransomware was responsible for the attack. While Rackspace had patched for an earlier related vulnerability, it did not apply a second patch published by Microsoft in time, which left it open to the attack. The infection was widespread across the service, with disruptions still being reported for roughly a third of customers over a week after the initial attack. Affected companies consisted primarily of small and medium-sized businesses, with the cybercriminals purportedly also accessing the Personal Storage Table of 27 out of 30,000 customers.

There was no evidence that the attackers viewed or misused the compromised emails or data. In response to the attack, Rackspace refused to pay the ransom, instead switching customers to Office365 environments and attempting to recover customer email history where necessary.

Event Narrative: Counterfactual Changes

For the Rackspace event, three 'impact' elements were considered to have the greatest counterfactual relevance:

Counterfactual 1: 'No Other Option'

Criteria	Element	Counterfactual Changes
Impact	Business Impact	No easy remediation Due to poor incident response plans, Rackspace presented no feasible redundancy options for impacted customers and was unable to migrate users to an alternative service.

Without another service to move users to (such as Office365), Rackspace would likely have had to rebuild the entire service from scratch, possibly incurring longer down times and business interruptions as impacted customers would be unable to continue business as usual during the recovery period.

Counterfactual 2: 'Zero-Day'

Criteria	Element	Counterfactual Changes
Impact	Propagation	Higher external proliferation rate Consider the effect of a zero-day vulnerability rather than a known vulnerability

Rackspace was able to mitigate a possible first wave of attacks by patching the first vulnerability. If the attack had exploited a zero-day vulnerability — i.e., there had been no warning or ability to prepare — the spread of infection could have been much worse. Coupled with an inability to 'fail over' to Office365, a faster infection rate could have completely wiped out the service offering for Rackspace. A similar example of such an event at a much smaller cloud services provider was the Cloud Nordic incident, which left the company on the verge of bankruptcy and left customers with no recovery options.

Counterfactual 3: 'Larger Footprint'

Criteria	Element	Counterfactual Changes
Impact	Impact Scaling	Spread to other services Consider the effects if the attack had impacted a broader range of Rackspace's services.

Hosted Microsoft Exchange services were only a small part of Rackspace's business in 2022. The apps and cross platform business unit accounted for roughly an eighth of its business revenue, with only a portion of that being Microsoft-based products. A more broadly targeted attack against multiple services using zero days could have affected closer to 300,000 customers, with much wider business interruption and data breach implications.

Counterfactual Loss Quantification

Table 2: CyberCube's counterfactual parameters and losses for Rackspace

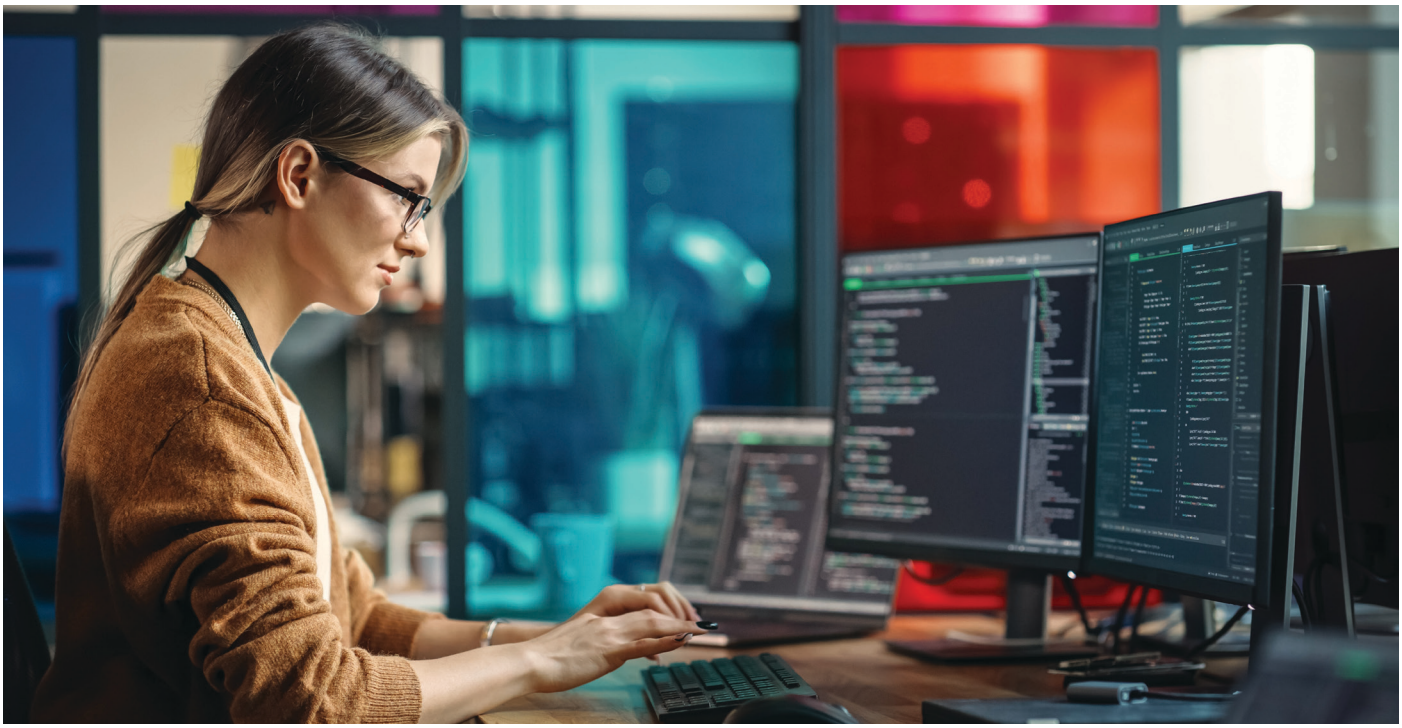
		Rackspace			
Criteria	**Counterfactual Analysis**	**Baseline**	**No Easy Switch Over**	**Higher External Proliferation Rate**	**Spread to Other Services**
Footprint	**# Customers (Companies)**	30,000	30,000	30,000	**300,000**
	Dwell time	**50%**	**85%**	**100%**	**85%**
	Vulnerability Rate	100%	100%	100%	**12.71%**
	Infection Rate	**100%**	100%	100%	**50%**
	SPoF Control Failure	**66.67%**	**83.34%**	**100%**	**30%**
	# Customers w/o Access	**10,001**	**21,125**	**30,000**	**34,862**
	Data Access Rate	0.09%	0.09%	**0.18%**	0.18%
	# Liability Breaches	**27**	**27**	**54**	**540**
	Needed Backups	**5%**	5%	5%	**25%**
	Impact Rate	31%	**45%**	45%	45%
	# Outage Customers	**155**	**475**	**675**	**3,922**
	Total Impacted Customers	**182**	**502**	**729**	**4,462**
Severity	Financial Claims Rate	9%	**13%**	**27%**	**37%**
	# Companies filing claims	**14**	**63**	**179**	**1,434**
	$M insured loss (conditional distribution)				
	5th	**$3**	**$27**	**$108**	**$1,718**
	50th	**$9**	**$56**	**$168**	**$2,148**
	95th	**$39**	**$108**	**$258**	**$2,660**

- Green and Blue rows represent commonly reported or known figures that tie the real world events to modelled events
- Green text represents known reported figures for these events (i.e. "baseline")
- Blue text represents changes in figures (model parameters) as each counterfactual step is added

https://status.apps.rackspace.com/index/viewincidents?group=2
https://www.crowdstrike.com/blog/owassrf-exploit-analysis-and-recommendations/
https://www.securityweek.com/rackspace-completes-investigation-ransomware-attack/

Understanding the Footprint

- SPoF Control Failure: This describes the percentage of systems where SPoF control failure over the course of the attack leads to impacted end users. For Rackspace this is combined with Dwell Time and calculated simultaneously to get to the known 10,000 affected customer count. In this case, Dwell Time is known to be a 50% rate due to only the first month's patch being applied and the second month's patch being left unapplied, meaning the dwell time could have been around 50% greater.
- Data Access Rate: This is the rate at which threat actors accessed the customer exchange backend table information compared to their total infection count (only 27 out of the 10,000 customers affected after a week of recovery had evidence of backend table access). This is likely due to a reduced focus from threat actors on data in lieu of an extortion focus. Increases to the reported number of customers with their proprietary data accessed would increase this rate. Increases in later counterfactual stages show higher rates of threat actor access, meaning more breach losses alongside business interruption.
- Needed Backups: Explores the proportion of customers who downloaded backups after the recovery process was completed and Rackspace restored access for the backups to be downloaded by customers. Rackspace data shows that only 5% of firms downloaded backups, demonstrating that their operations were likely back up and running from the moment that they had access to their new email. This means that these customers had either already downloaded their backups from a previous month or did not require them for business continuity to be restored. As the final counterfactual change shows, the need for backups is assumed to be higher when more business critical services (other than email) are affected.
- Financial Claims Rate: The percentage of companies with both Insurance and an impact to the degree that they need to file a claim.



Conclusions

In this paper, Gallagher Re, with the support of CyberCube, has demonstrated through worked examples that a counterfactual analysis doesn't have to be a significant undertaking but can produce highly relevant insights and variations of stress tests that can be adjusted depending on internal risk appetite and portfolio composition. Even altering only a few input assumptions can result in significant variation in losses.

In our Kaseya example, the baseline insured loss was just $230Mn even in the tail, at the 95th percentile, but in the 'wiperware' counterfactual scenario, that figure drastically increases to over $4Bn. In the Rackspace case study, a baseline 95th-percentile loss of $39Mn becomes a loss of $2.7Bn in the scenario where the attack impacts a broader suite of the company's services.

These downward counterfactuals of past events can help insurers form a deeper, more evidenced view of the risk exposures in their portfolio — and since they are both quantitative and intuitive, they can also help communicate those views to internal and external stakeholders more effectively. This is becoming a critical requirement for portfolio growth and accessing capacity in the (re)insurance markets.

We hope that the illustrations provided in this paper encourage others to conduct their own exercises. The ability to analyze historic events in the context of current technological and threat conditions will be a vital tool for insurers in differentiating themselves from their peers, and maintaining or gaining vital underwriting capacity.

If you wish to discuss any matters in this paper further, please contact

Simon Heather
Head of Cyber Catastrophe Modelling
Gallagher Re
simon_heather@GallagherRe.com

Sioned Bentley
Senior Cyber Risk Consultant
Gallagher Re
sioned_bentley@GallagherRe.com

Jon Laux
VP Analytics
CyberCube
jonl@cybcube.com

Josh Knapp
Principal, Cyber Risk Modeling
CyberCube
joshk@cybcube.com

CyberCube: Using Counterfactual Analysis for Model Development

Anyone can understand hurricanes, earthquakes, floods, and wildfires. We can all conceptualize them, even if we haven't experienced them firsthand. But do we understand what a major cyber attack looks like? Feels like? Few cyber events so far have 'made landfall' in a meaningful way, and a focus only on the realized losses from past events can make it challenging to conceptualize a true 'worst-case' scenario. Events like Not Petya or WannaCry seemed out of the realm of possibility for some people just decades ago. Just as hurricanes and wildfires have recalibrated industry models in recent decades, cyber events can reset our paradigm of understanding. This recalibration often happens at a faster pace than physical perils. Moreover, it is often difficult to grasp the digital realities of cyber-catastrophic events.

There is often no warning, no physical damage, and a lack of a visual aftermath. This highlights a key difference in the cyber peril: cyber risks are complex and dynamic, arising in many forms, and evolving quickly. Experience shows us that cyber event losses and characteristics are nonlinear, meaning any one change to a past event could have meant it never happened in the first place, or that it was orders of magnitude worse. In US Wind terms, it might be like a tropical depression having the potential to become a major hurricane — suddenly and without warning, just miles from land. Or a Category Five hurricane that no one knew about barreling towards a major metropolitan area before vanishing into thin air.

While it is generally understood that cyber events could result in worse losses than in the past, how much worse is often hard to grasp. For this purpose, **CyberCube has embraced counterfactual analysis as a valuable approach**. Counterfactuals require looking at the past differently: not only what did happen, but also what could have happened or nearly happened.

CyberCube has used counterfactual analysis in numerous ways to enhance and validate our models. Key areas include:

- Model parameter validation of simulated events by studying real-world event characteristics,
- Real-world infection rates, response times, and financial impact,
- Simulating changes to real-world events as compared to permutations of events within our event catalogue,
- Testing feature additions against historical and theoretical events, and
- Testing market realities against historical and theoretical events.

Through these exercises, invaluable insights have been used to enhance the applications of our models. Counterfactuals have served as an important tool to translate between our models and the real world. The ability to tether model parameters, changes, and features to aspects of real-world events allows for great understanding and improved adoption of models in cyber insurance. By bridging the gap from what has happened to what could happen, models can be understood, relied upon, and utilized to greater effect when planning for the evolving threat landscape.

This approach provides the ability to look at tail events relative to certain historical events. By using counterfactuals in this way, we can understand cyber scenarios in a more tangible way — a tail event might only be two or three steps removed from one that the industry has seen. Indeed, we have seen this to be the case.

Learn more about our client-focused, collaborative approach.
Connect with us today at **GallagherRe.com**.

It's the *way* we do it.

Gallagher Re