GuyCarpenter

Cyber Event Analysis | August 1, 2024

A CLOSER LOOK: UNVEILING THE GLOBAL IMPACT OF CROWDSTRIKE EVENT

CrowdStrike, a leading cybersecurity technology provider, offers a range of products and services, including endpoint detection and response (EDR). EDR monitors traffic passing through computer systems to protect against malicious files, viruses and malware. In its last earnings report, CrowdStrike reported a total of nearly 24,000 organization customers, including nearly 60% of the Fortune 500.

On July 19, at 04:09 am UTC, CrowdStrike released a "Rapid Response Content" update to its EDR tool dubbed “Falcon,” sitting on Microsoft Windows devices. CrowdStrike uses Rapid Response updates to adapt to the changing threat landscape quickly. Unfortunately, this update contained a software coding flaw that caused Microsoft devices to crash, leading to the infamous "blue screen of death." CrowdStrike promptly reverted the update and introduced a fix, but the impact was significant.

The CrowdStrike event highlights the potential severity of digital supply chain interconnectedness, as it disrupted not only CrowdStrike's customers but also propagated through third-party networks, impacting the resilience of seemingly unrelated industries. However, in the immediate aftermath we observe that insurers are carefully considering the implications of this event and continuing to support their clients with unchanged coverage, thus demonstrating the resilience of the cyber insurance market.

Following this incident, Guy Carpenter has estimated the losses and evaluated the implications for underwriting considerations and catastrophe risk management.

Measuring the Impact

Ultimately, while the millions of affected devices represent only a small percentage of Microsoft devices, the flawed update caused operational disruptions globally. More than 7,000 flights were canceled or delayed over several days, and disruptions were felt in critical infrastructure sectors such as healthcare, retail, financial services and hospitality. Estimates of the impact are still evolving. At this point, many insureds have filed notices of circumstances, and it is still early in the claims process.

While some cyber catastrophe model vendors contemplate malicious events only, others have accidental event scenarios in their catalogue. These events are not directly comparable to the CrowdStrike outage, but they can form a basis to derive a loss estimate. Notably, the profile of accidental outages known as System Failure lacks many costs that rapidly ramp up in the case of malicious triggers, such as forensic expenses, breach counsel, data restoration and extortion costs.

CrowdStrike’s outage will have insurable loss by triggering some coverage sections, but the non-malicious nature of the disruption limited the breadth of impact a malicious event could have created.

Using this breakdown of impact on coverages, Guy Carpenter developed a 5-step modelling approach, which leverages leading cyber vendor tools, to model the potential loss of the CrowdStrike Falcon outage:

1. Analyzing vendors’ catalogues to identify cyber events comparable to the CrowdStrike event.
2. Assessing the gap between the identified cyber events in Step 1 and the CrowdStrike incident (e.g., outage duration, malicious versus accidental intent, footprint).
3. Adapting the retained event(s) to mimic the CrowdStrike outage by:
    a. Capturing the technology landscape. In this instance, we contemplated specific versions of Microsoft operating systems and servers in line with the versions that were impacted by the CrowdStrike outage.

Table 1: CrowdStrike Outage Loss Estimate

Vendor	CrowdStrike Outage Loss Estimate
CyberCube[1]	$372 million – $1.4 billion (2–6%)
Guidewire Cyence[2]	$1 billion – $3 billion (6–19%)
Guy Carpenter	$300 million – $1 billion (2–6%)

1. These figures exclude loss estimates relating to CrowdStrike insurance tower as quantified by CyberCube. When included, the range becomes $400 million – $1.5 billion.

2. These figures are economic estimates.

Source: Guy Carpenter

   b. Deriving the corresponding footprint in line with CrowdStrike Falcon market and Microsoft solutions market shares.

   c. Focusing on events with spreading rates and outage durations close to what we observed post CrowdStrike incident.

4. Focusing on Business Interruption and Contingent Business Interruption coverages only to account for the accidental nature of this outage in contrast to its malicious counterpart.

5. Computing the losses with different intensities to capture moderate to extreme variations this incident can take.

In addition, pursuant to the vendor guidance for quantifying the CrowdStrike Falcon outage, Guy Carpenter evaluated catalogue scenarios affecting similar technologies and introduced bespoke scalars to adjust the footprint and severity.

We collated the various loss estimates from the different vendors as well as Guy Carpenter's own estimate. The table below shows the different estimate in absolute and loss ratio terms based on Guy Carpenter's $15.8 billion gross premium estimate for the cyber insurance industry.

According to Guy Carpenter's estimates, less than 1% of companies globally with cyber insurance were impacted. With a quickly introduced fix, many organizations had the opportunity to mitigate the outage before the waiting period expired for business interruption claims. Typically, those range between 4 to 12 hours in cyber insurance policies. As a result, the likely insured loss is between $300 million and $1 billion. Guy Carpenter's findings align with the conclusion that this event would not result in a material loss for most insurers, although this could change based on the wordings adopted by carriers, concentration of underwriting within affected industry sectors, and uptake of System Failure coverage.

Table 2: Assessment of Coverage Scope for CrowdStrike Outage

Cyber Product Coverage	Materiality	Rationale
Forensic	Very low	CrowdStrike identified the issue and released a fix within approximately 1 hour of the outage occurrence.
Notification	Very low	No personal data subject to unauthorized access to require notification and privacy services required by law and regulation.
Data restoration	Very low	No corruption or encryption of data.
Business Interruption (System Failure)	Medium to High	Main driver of potential losses. If System Failure coverage was extended onto Business Interruption coverage, then the materiality could be High. Note System Failure may be sublimited.
Contingent Business Interruption (Contingent System Failure)	Medium to High	Similarly to business interruption costs, organizations that relied on other companies affected by CrowdStrike could be impacted downstream if Contingent System Failure was extended on the policy. Since the outage was resolved for many quickly and it was non-malicious, this is less likely to have a High materiality.
Legal	Low	Legal actions potentially limited to parties central to the loss events.
Extortion	NA	NA
Other	Very low	Other minimal costs may be triggered, such as reputational damage from customer churn.

Source: Guy Carpenter

Underwriting Considerations

Had the event been malicious, the impact would be far greater. Guy Carpenter estimates that a ransomware attack that directly impacts a widely used operating system could have a total impact between $600 million and $2 billion in insurable loss.

If the outage remains limited in scope, it will give greater perspective to underwriting for Business Interruption and System Failure. This technology outage highlights the increased risk faced by organizations that rely on widely deployed software running on a dominant operating system provided by commonly used vendors. Impacted organizations benefitted from a quick response and transparency around the issue. CrowdStrike announced measures to mitigate the risk of future similar disruptions, and this event should serve as a learning moment for all technology providers and their clients.

Underwriters must consider the unique circumstances that led to this outage for developing future risk appetite. First, in this instance, the vendor had high-level privileges to communicate directly with sensors linked to the operating system software. Importantly, most vendors do not have this level of access and, therefore, cannot directly impact the operating environment. This prioritization limits the ability of most software updates to disrupt the environment, which keeps operations more stable and reduces the potential frequency for similarly caused widespread system failures.

Second, automated content updates provide significant value for EDR tools. Regularly providing cybersecurity product updates protects against evolving malicious activity. Delaying such content updates would slow down behavior-based detection and increase the threat of malicious activity, including targeting zero-day vulnerabilities. Accordingly, vendor-initiated system failures are challenging to underwrite.

Ultimately, as long as software and updates remain flawed, insurers will need to consider how technology poses the greatest risk to interconnected failures and how insureds can establish resiliency from such failures. Evaluating how technology dependencies and digital supply chain risk differs by industry and size segments within a portfolio may insulated outsized impacts. The CrowdStrike outage also sheds light on the effectiveness of Waiting Hours retentions within Business Interruption coverages.

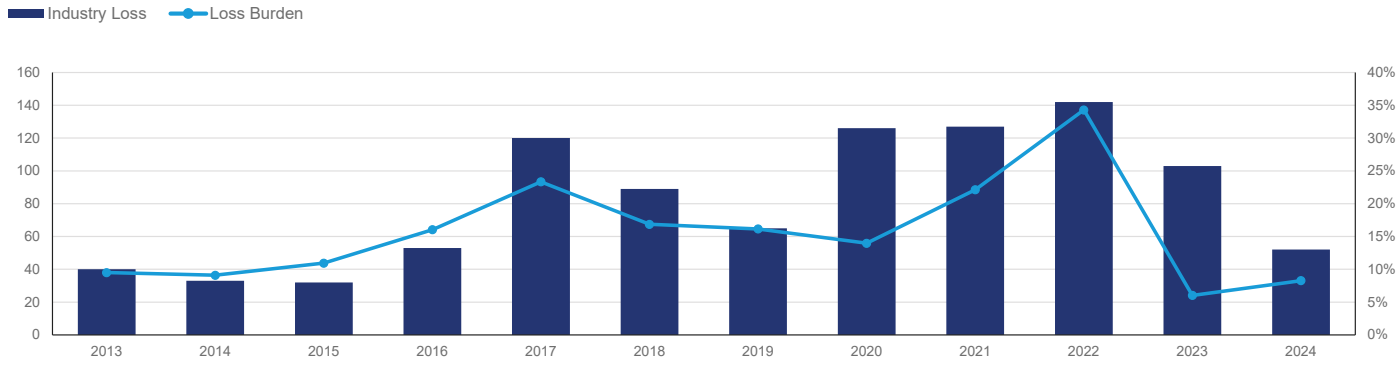
Each market loss, especially headline-grabbing events, sharpens the understanding of nuances in quantifying cyber exposure and systemic threats while testing the efficacy of coverage and relevancy of the products. As the market matures, these shots across the bow of sizeable but manageable cat events refine how to best protect capital at each step of the insurance value chain without a doomsday loss quantum.

Shifting View of Cat Risk

As the cyber market continues to mature, the potential for cat events has influenced scenario modeling and reinsurance purchasing trends. However, given the events of the past 18 months, the industry should re-evaluate its perspective of risk and consider the impact of frequency losses alongside the market moving systemic risks. Rather than bracing for the single super cat, perhaps the market should be more concerned with the growing litter of “Kitty Cats”—mid-size events that meet the criteria for a cat loss, but at a smaller scale.

Since May 2023, the cyber market has experienced five Kitty Cats—MoveIT, Change Healthcare, CDK Global, CrowdStrike, and Snowflake—all of which were headline news. While these losses have had limited impact

Figure 1: Loss Burden of Largest Individual Property Claim by Year



Source: Guy Carpenter

individually, when aggregated into a single treaty period, they could generate a >10% loss ratio impact to the industry, which is more in line with the expectation for a single super cat.

This aligns with cyber catastrophe modeling and scenario analysis, which have focused on events contributing double-digit impacts to loss ratios. As the industry grows and loss coding and reporting continues to improve, market understanding around individual loss burdens from leading events will provide more insight to help manage portfolio aggregation and cat risk. Using the experience from the property world where large individual cat events have contributed 5%-40% to the annual loss burden, the expectation that the cyber market may have to weather several such events in the course of an underwriting year becomes clear.

Kitty Cat events are hard to predict and, therefore, hard to model accurately compared to their super cat counterparts. This is further corroborated as vendor models diverge further in lower return periods than in the tail. Some can be approximated using modified vendor scenarios, but there are no placeholder scenarios available to approximate the loss. As the industry further improves loss coding and reporting for cat events, its understanding of individual loss burdens from leading events will provide clarity on how to best manage losses from these events.

How Guy Carpenter Can Help

The CrowdStrike Falcon incident had a global impact, causing operational disruptions across various sectors. While the exact losses are still being determined, estimates suggest a sizable but manageable insured loss.

Guy Carpenter analytics has provided perspective on the CrowdStrike Falcon incident with a multi-view perspective including:

- Single Point of Failure (SPoF) analysis using tools licensed from KYND and CyberCube that estimate dependencies on CrowdStrike Falcon to see where losses may emerge;
- Modeled View of Loss by leveraging a multi-vendor analysis that quantifies the CrowdStrike financial impact associated with insurer-specific portfolios; and
- Insights from a cybersecurity, claims and underwriting standpoint provided across Marsh McLennan.

These capabilities address portfolio nuances, with the ultimate objective of supporting our clients with capital protection solutions. In addition, Guy Carpenter's proprietary CatStop+ product maintains the flexibility to respond to risk from emerging events, as well as the unfolding uncertainty around cat losses.

Guy Carpenter's Cyber Center of Excellence is poised to help our clients with tools and expertise to navigate these challenges and optimize their reinsurance strategies.

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.