





Cyber Event Analysis | July 19, 2024

A GLOBAL OUTAGE WITH WIDESPREAD IMPACT

Incident	Revealed	Impacted Parties	Cause
 <p>Global Outage</p>	 <p>July 19, 2024</p>	 <p>Microsoft Users</p>	 <p>Falcon Sensor Software Update</p>

On July 19, at 04:09 am UTC, cybersecurity company CrowdStrike released a software update for its Falcon Sensor product, which is designed to detect malicious threats at a computer system's endpoints. The update resulted in the widespread crashing of computers using Microsoft Windows operating systems. Thus far, the update has only affected Microsoft users, and there has been no report of other operating systems being impacted. The system failure caused by the CrowdStrike update impacted a broad cross-section of industries, including airlines, banks, retailers, hospitality and more.

The event demonstrates a single point of failure for a complex, global information technology supply chain. Cyber insurers should use this event to evaluate policyholder supply chain dependencies, assess the potential for aggregation across commonly used technologies, and recalibrate risk tolerances accordingly.

Loss Components

Cyber insurance provides for broad coverage of business interruption resulting from network outage. The trigger for this coverage includes **System Failure** resulting from non-malicious acts, including human error. That coverage extends to **Contingent Business Interruption (CBI)** caused by an outage of a vendor on which an insured relies to operate its network.

Critical for evaluating network interruption claims will be the policy waiting period for which the network must be impaired before the policy responds. Typical cyber waiting periods vary depending on industry class and organizational size with 4-12 hours being most common.

CBI losses arising from a widely deployed technology present reinsurers with an acute risk for unexpected aggregation. Technologies with large market shares create potential single points of failure that can lead to systemic events yielding claims from a large number of insureds.

Modeling The Incident

While modeling scenarios do not account specifically for widespread outages due to software updates, there are sufficient analogous scenarios for estimating losses from the event, including business interruption and extra expense. These scenarios typically contemplate companies losing control over IT-related services, the impacts on customers and sales, and the potential for slow recovery.

While actual losses will vary from modeled instances based on the specific circumstances, such scenarios can establish a directional foothold for cedents to address systemic exposures. Guy Carpenter is currently engaged with the cyber catastrophe vendors for their analysis of this event and is conducting our own view to share with clients.

Impacts On Cyber Reinsurance

System failure losses will be in scope for traditional proportional and aggregate structures, which respond to all causes of loss. In recent renewal cycles, buying behavior selectively shifted toward targeted catastrophe covers, many of which respond to specifically defined catastrophic scenarios. Event-based products and the definitions behind them are unique to the cedent's view of risk and how coverage was negotiated. Recoveries from event-based products will differ based on how each underlying wording differentiates coverage between malicious and non-malicious cyber incidents. As this incident progresses, Guy Carpenter will clarify its impacts on the assumptions around tail risk and the overall USD 15.5 billion global cyber industry moving forward.

Beyond Cyber Insurance

Given the magnitude and scope of this outage, we may see consequences that affect product lines beyond cyber risk, most prominently directors & officers (D&O) and property/casualty (P&C).

- **D&O.** We may see implications on the D&O towers for companies both involved in or impacted by today's incident. In general, a 10% intraday stock drop for a publicly traded company may incentivize the plaintiffs' bar to file a class action lawsuit. Subsequent share price moves and any ultimate recovery may also impact the likelihood of litigation. Historically, securities class

actions arising from technology incidents have fared poorly. In addition to securities class actions, companies that are either involved in or impacted by the event may face increased exposure if they struggle to restore operations and may face shareholder derivative suits alleging the board's breach of fiduciary duty.

- **P&C.** With the continued integration of information technology and operational technology, insurers must also consider the physical consequences that may arise from technology failures. Potential exposure for P&C policies will depend on how insurers address cyber as a peril and whether the policy includes a "silent cyber" exclusion. Policies remaining silent on cyber risk may be exposed to ensuing bodily injury or property damage as a result of cyber-related system failure.

Guy Carpenter supports our clients through complex market developments. Our Cyber Center of Excellence analyzes reinsurance event language and stress tests its efficacy against potential cyber losses. The GC CyberExplorer® DataLake provides our clients with up-to-date intelligence for assessing the various dimensions of technology events, including software failure and network outages. Broad impact and large-scale events are part of developing a thriving insurance and reinsurance marketplace. Assessing events like today's outage matures the view of catastrophe potential and advances structural considerations for protection.

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.

Guy Carpenter & Company, LLC provides this report for general information only. The information contained herein is based on sources we believe reliable, but we do not guarantee its accuracy, and it should be understood to be general insurance/reinsurance information only. Guy Carpenter & Company, LLC makes no representations or warranties, express or implied. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such. Statements concerning tax, accounting, legal or regulatory matters should be understood to be general observations based solely on our experience as reinsurance brokers and risk consultants, and may not be relied upon as tax, accounting, legal or regulatory advice, which we are not authorized to provide. All such matters should be reviewed with your own qualified advisors in these areas.

Readers are cautioned not to place undue reliance on any historical, current or forward-looking statements. Guy Carpenter & Company, LLC undertakes no obligation to update or revise publicly any historical, current or forward-looking statements, whether as a result of new information, research, future events or otherwise. The trademarks and service marks contained herein are the property of their respective owners.

©2024 Guy Carpenter & Company, LLC. All rights reserved.