# CYBER UPDATE

## CrowdStrike, the Most Important Cyber Accumulation Loss Event Since NotPetya, Highlights Single Points of Failure

WINTERS-OLIVER
INSURANCE AGENCY, INC.

In what is being called "the most important cyber accumulation loss event since NotPetya," the July 19, 2024, global technology outage (CrowdStrike) will produce scores of insurance claims across a range of policies, test cyber policy wordings, and sharpen the industry's focus on single points of failure.

Caused by a flawed software update from cybersecurity firm CrowdStrike and impacting a reported 8.5 million devices running Microsoft's Windows system, the outage brought businesses around the world to a digital halt. Airlines, health care facilities, government agencies, emergency response services, banks and businesses across multiple industries faced system crashes and a "blue screen of death."

CrowdStrike quickly announced that it was a defect in an update for its Falcon endpoint detection and response (EDR) platform that caused the outage, not a cyberattack.

"All of CrowdStrike understands the gravity and impact of the situation. We quickly identified the issue and deployed a fix, allowing us to focus diligently on restoring customer systems as our highest priority," said George Kurtz, the firm's CEO, in a statement. He also warned affected organizations that "adversaries and bad actors will try to exploit events like this" and to stay vigilant against social engineering scams attempting to leverage the outage.

However, experts also say the recovery process could take time since the fix requires access to Windows Safe Mode and may be challenging to implement remotely.

The outage has already drawn scrutiny from federal lawmakers, with members of the U.S. House of Representatives calling on Kurtz to testify before the House Homeland Security Committee.

### Cyber Insurance Implications

Early estimates suggest the insured losses from the CrowdStrike outage may hit the mid to high single-digit billions, according to commentary from Fitch Ratings.

While an insured event of that size wouldn't likely have a "material" impact on global insurers and reinsurers, the claims process will be lengthy with inevitable litigation.

The firm highlighted cyber, business interruption and contingent business interruption (CBI) as the most impacted insurance coverages. However, it cited the potential for payouts on travel insurance, event cancellation and technology errors and omissions.

Cyber insurance professionals have braced for incoming losses for business interruption stemming from the event. According to industry experts, nonmalicious acts (including human error) can trigger system failure coverage, which can extend to CBI cover. Noncyber policies could also be affected, depending on how cyber is handled as a peril, including directors and officers liability coverage.

Policies that do not address cyber risk may be vulnerable to resulting bodily injury or property damage from cyber-related system failures. Additionally, companies involved in or affected by such events might encounter heightened exposure if they have difficulty restoring operations. This could lead to securities class actions and shareholder derivative suits alleging a board's breach of fiduciary duty.

Industry experts agree that insurance recovery from the CrowdStrike event will hinge upon cyber policy wordings and waiting periods before business interruption cover kicks in. Waiting periods usually range from eight to 12 hours but can be as short as six hours or as long as 24.

Aon's Reinsurance Solutions team commented in a brief, "This is likely to be the most important cyber accumulation loss event since NotPetya in 2017. However, the overall loss quantum is currently uncertain … The extent to which this is a covered event for insureds will vary."

The broker said it analyzed cyber policy wordings and found "a range of approaches" to system failure and nonmalicious events. Some carriers offer it as a standard cover, while others do not.

Aon said it expects the event to "trigger greater attention to system failure coverage grants and business interruption waiting periods." It could also impact event definitions used by insurers, reinsurers, and the industry's burgeoning cyber catastrophe bond market.

Cyber modeling firm CyberCube has dubbed the event "CrowdOut" and highlighted the importance of understanding single points of failure (SPoF). The sphere of companies affected by the event not only includes CrowdStrike customers, but other organizations that are SPoFs in their own right.

"With its global position in cybersecurity, CrowdStrike's customer base includes many other organizations that CyberCube identifies as SPoFs. Companies relying on one of these SPoFs may be secondary victims of the event, even if they do not use CrowdStrike and Windows directly," CyberCube said in a blog post.

The event "mimicked a supply chain incident, causing cascading and widespread disruptions among interconnected systems," said Damini Mago, assistant director of product management for cyber at Moody's RMS, in a blog post.

"The recovery process could extend over days or weeks, with the potential to cause significant operational downtime," Mago warned, noting that since insurers often require EDR policies as a condition of coverage, CrowdStrike's customer base is more likely to be insured.

"Insurers could see that their incident response and claims handling teams are stretched thin given the scale of this incident, as the number of enterprises impacted and how they were impacted becomes clearer in the next few days," she added.