



---

ICE'S DATA BREACH CASE STUDIES

# CrowdStrike

# CROWDSTRIKE OUTAGE COULD COST CYBER INSURERS \$1.5 BILLION

The triggered by a faulty CrowdStrike software update on July 19 could lead to cyber insurers paying out up to \$1.5 billion in compensation.

That's the conclusion of cyber risk analytics platform CyberCube, which in a Thursday report said the insurer losses range from \$400 million to \$1.5 billion. Those figures represent 3% to 10% of the \$15 billion in global cyber premiums held today.

The final insurance payout total will need time to emerge. "Determining final losses for the industry is likely to be a lengthy process because cyber insurance policy language is not standardized," Moody's Reports said in a Monday report. "It will take time for insurers to determine which customers suffered losses from the outage, and whether those losses are covered."

Most claims will center on losses due to "business interruption, which is a primary contributor to losses from cyber incidents," it said. "Because these losses were not caused by a cyberattack, claims will be made under 'systems failure' coverage, which is becoming standard coverage within cyber insurance policies." But, not all systems-failure coverage will apply to this incident, it said, since some policies exclude nonmalicious events or have to reach a certain threshold of losses before being triggered.

The outage resembled a supply chain attack, since it took out multiple users of the same technology all at once - including airlines, doctors' practices, hospitals, banks, stock exchanges and more.



Cyber insurance experts said the timing of the outage will also help mitigate the quantity of claims insurers are likely to see. At the moment CrowdStrike sent its update gone wrong, "more Asia-Pacific systems were online than European and U.S. systems, but Europe and the U.S. have a greater share of cyber insurance coverage than does the Asia-Pacific region," Moody's Reports said.

The outage, dubbed "CrowdOut" by CyberCube, led to 8.5 million Windows hosts crashing to a Windows "blue screen of death" and then getting stuck in a constant loop of rebooting and crashing. Many IT teams, with help from CrowdStrike and Microsoft, have been working nonstop since then to recover affected systems.

By Thursday, CrowdStrike reported customers had successfully restored 97% of affected Windows PCs, servers and virtual machines.

Cloud outage risk modeler and underwriting agency Parametrix Solutions said the outage directly affected one-quarter of the 500 most profitable publicly traded U.S. companies. Those corporations will collectively see \$5.4 billion in direct losses as a result, it forecast (see: CrowdStrike Outage Losses Will Hit Healthcare, Banking Hard).

That estimate doesn't include expected "very significant intangible losses" for Microsoft, Parametrix said, stating that those remain difficult to predict.

Moody's Ratings expects the CrowdStrike outage to "spur demand for cyber insurance" by new policyholders, as well as drive the market to further refine its "cyber modeling" to take into account not just ransomware and data breaches but more widespread outages such as the CrowdStrike disruption.

Unlike the SolarWinds supply chain attack or last year's attacks on online Microsoft Exchange servers, the outage didn't stem from malicious activity. It wasn't combined with crypto-locking malware, extortion, cyberespionage or other nefarious activity. "Had this event been a malicious attack that deployed ransomware bricking a large number of computer systems the losses would have been far worse," CyberCube said.

Even so, the outage highlighted "the broad risks posed by a single point of failure and the degree to which many segments of the economy are interconnected and interdependent," Moody's said. Rectifying those problems won't necessarily be an easy task, but it should lead to much better overall cybersecurity resilience, experts say (see: CrowdStrike, Microsoft Outage Uncovers Big Resiliency Issues).

CrowdStrike last week released a preliminary report on the outage, which it said occurred because its faulty code-testing procedures failed to prevent a bad software update from being distributed to customers' Falcon endpoint security agents. The company pledged to overhaul its testing practices and to make a number of other changes designed to prevent a recurrence.



888-423-4801



[www.iceconsulting.com](http://www.iceconsulting.com)



[info@iceconsulting.com](mailto:info@iceconsulting.com)

Part of the problem is that a third-party Windows security software application was able to send its Windows host into a nonstop reboot loop without the operating system being able to automatically recover. Software experts say that problem doesn't just involve CrowdStrike but is a risk posed by most Windows endpoint security - aka antivirus or anti-malware - tools because they rely on kernel-level drivers that run with the greatest possible privileges on a system.

Microsoft hasn't pledged to overhaul Windows to eliminate that requirement but it will "work with the anti-malware ecosystem" to help it make its approaches more secure, said David Weston, Microsoft's head of enterprise and OS security, in a Saturday blog post.

This will include "providing safe rollout guidance, best practices and technologies to make it safer to perform updates to security products," as well as new Windows features designed to reduce "the need for kernel drivers to access important security data," he said.

## PROTECTING YOUR ORGANIZATION

Security Operation Centers as a Service (SOCaaS) are on the rise, especially in the life science sector, a prime target for cyber threats. Accenture forecasts potential losses exceeding \$657 billion for life science firms in the near future.

SOCaaS offers your company a dedicated team of cybersecurity specialists who proactively detect and combat cyber threats round the clock through a SIEM platform. Service providers can swiftly deploy a team to shield your organization within a week's time. The cherry on top? All this comes at a fraction of the cost of establishing an in-house cybersecurity department.

As a Managed Cybersecurity Provider, ICE offers this service. For more information, feel free to reach out to us today!



888-423-4801



[www.iceconsulting.com](http://www.iceconsulting.com)






[info@iceconsulting.com](mailto:info@iceconsulting.com)




**ICE Consulting, Inc**  
**Managed Cybersecurity Provider**



 888-423-4801  
 [info@iceconsulting.com](mailto:info@iceconsulting.com)  
 [www.iceconsulting.com](http://www.iceconsulting.com)



 888-423-4801

 [www.iceconsulting.com](http://www.iceconsulting.com)

 [info@iceconsulting.com](mailto:info@iceconsulting.com)