Cyber

Client alert

CrowdStrike Global Outage

CrowdStrike global technology outage underscores fragility of global IT systems

Organizations across a wide range of industries around the world, including airlines, banks, telecommunications, media and healthcare have been grappling with the impacts of a global technology outage attributed to CrowdStrike, a cybersecurity firm whose software is used by these industries to protect against hackers and outside breaches.

Microsoft estimate that 8.5 million Windows devices have been impacted. CrowdStrike, in a statement issued on July 21 confirmed that a "significant number" of those devices are now back online and operational. Earlier, on July 19, Crowdstrike reported that the cause of the outage was attributable to a "defect found in a single content update for [Microsoft] Windows hosts" and "not a security incident or cyberattack."

While Australian businesses were the first to identify problems, the outage quickly spread to other regions of the world. The outage caused hundreds of flights to be grounded, cancelled or delayed. Many doctors at hospitals that relied on the CrowdStrike system for scheduling were forced to postpone or cancel surgeries, other shipping and production companies like General Motors also experienced disruption to sales and scheduling, while some live broadcasts went dark. Further, the outage affected 911 lines in multiple states, according to the U.S. Emergency System. Finally, certain banks have reported delays in processing trades because bankers were unable to log into their networks. Further consequences of this widespread global incident will no doubt continue to be reported.

Cyber Insurance Implications

Assuming CrowdStrike's assessment that the outage was not caused by security incident or cyberattack is unchanged, when viewed through the prism of cyber insurance, this incident will likely be considered a system failure (commonly defined in many cyber policies as an unintentional and unplanned failure of a computer system or network). Equally, the software error (subject to the specific facts) could fall within scope of an operational error or programming error where such events are covered under the policy. When evaluating coverage for business interruption loss and extra expense under your cyber insurance policy, it is important to consider the following:

1. **What coverage is available?** Many cyber policies offer full or sub-limited coverage for business interruption loss and extra expense caused by an interruption on the insured's own network as well as the networks of third party providers (as defined). There are two obvious questions to be addressed: (1) does CrowdStrike's software, under the terms and conditions of the cyber policy, fall within scope of the insured's network or the network of a dependent business or outsource provider? and (2) once, question 1 has been determined, how does the policy respond to a system failure/operational or programming error impacting the insured's network or the network of such provider?

2. **What is the waiting period and when will it begin to run?** In other words, how long does the insured event need to last for the business interruption coverage to be granted? Whether or not the insured event has exceeded the waiting period will be subject to the specific language in the policy.

3. **How will the business interruption loss be calculated?** Business interruption loss calculations can vary significantly between policies. For example, some policies calculate the loss starting when the network was first interrupted once the waiting period has been exceeded (known as the 'franchise basis') whereas other polices only indemnify loss incurred after the waiting period has expired. It is also important to keep an eye on whether the calculation of loss will end when the business's network is physically back up or when the insured restores its business operations to the same or similar conditions that existed prior to the outage.

4. **Understanding your loss:** Your broker can assist you in determining what business interruption coverage may be available to you based on the above considerations and how to engage a forensic accountant to calculate your loss. It is important to:
   a. keep track of impacted systems, the date each system is partially and fully restored, and the impact each system's outage has on your operations and revenue generation.
   b. keep notes on any manual workarounds your organization needs to implement, or any incremental hours your employees work above and beyond what they would normally work in order to continue business operations.
   c. Finally, keep a detailed narrative of events since the claims process can be lengthy. Sometimes during the claims process, employee turnover can occur, and information could potentially get lost if you don't maintain detailed records.

5. **Should I notify my insurers?** We encourage any client who has (or suspects they may have) been impacted by this event to contact their WTW broking team to discuss notifying the incident in line with their policy terms and conditions. Notification is a threshold requirement for triggering insurance coverage under many insurance policies and should be investigated and completed quickly.

What next?

While the initial issue has been identified and isolated, and a fix has been deployed, the ongoing disruption from this incident will continue over the coming weeks. In the immediate aftermath, cyber criminals will seek to exploit the situation using phishing emails purporting to be from CrowdStrike or Microsoft. It's important that organizations and their staff continue to remain vigilant for any suspicious communications.

From a broader perspective, identifying, understanding and managing cyber/network related vulnerabilities should be part of the operational resilience strategy of every organization - what the CrowdStrike issue reinforces is that while an organization can develop an effective cyber security strategy, the dependency on third parties is not a risk that is easy to manage. Preparing in advance is one of the best ways to reduce the cost of dealing with a major cyber/network incident similar to the one described above. All insurers now are insisting businesses meet specific cyber security criteria to be eligible to purchase cyber insurance.

Please contact us to see how we can assist you in tailoring your cyber risk management approach and coverage to suit your risk profile and business needs.

Contacts

Australia
Benjamin Di Marco
Head of FINEX Cyber & Tech
Direct: +61 478 312 988
benjamin.dimarco@wtwco.com

Asia
Jennifer Tiang
Head of FINEX Cyber & Tech
Direct: +65 8441 7344
jennifer.tiang@wtwco.com

Canada
Michélle Lawson Hughes
Head of FINEX Cyber & Tech
Direct: +1 416 646-3161
michelle.lawson@wtwco.com

Great Britain
Glyn Thoms
Head of FINEX Cyber & Tech
Direct: +44 7985 164 928
glyn.thoms@wtwco.com

LATAM
Rodrigo Flores
Head of FINEX Cyber & Tech
Direct: +52 55 4383 8517
rodrigo.flores@wtwco.com

Western Europe
Laure Zicry
Head of FINEX Cyber & Tech
Direct: +33 1 55 91 30 28
laure.zicry@wtwco.com

North America
Jason Warmbir
Head of FINEX Cyber & Tech
Direct: +1 312 607 0096
jason.warmbir@wtwco.com

Global
Peter Foster
Chairman, Global FINEX Cyber and Cyber Risk Solutions
Direct: +1 617 901 8174
peter.foster@wtwco.com