CISO Cross-Industry

Expert Exchange

Q4 Executive summary
October 22, 2024

kyndryl

Overview

In this Expert Exchange session, several CISOs convened to discuss security and resilience topics following the CrowdStrike incident. The agenda was created based on advance interviews with participants

Host

Michael Restivo, Kyndryl, US Vice President – Security and Resiliency

Key topics

The CrowdStrike incident and its impact

- The group members shared how the July CrowdStrike incident affected their company operations, with the level of impact depending on CrowdStrike's footprint. One member described how they were back online by 3 p.m. that day, but for others, it took 12 hours or more to get everything back up and running. Even those not partnering with CrowdStrike directly may have been affected by the outage because the incident had a cascading "ripple effect" throughout companies worldwide.

- Several members stressed that the incident shined a spotlight on the need for resilience throughout company security systems and operation software. While the CrowdStrike breach was not a cybersecurity attack, it had similar impacts that would fit into the playbook for cyber-attack response and resiliency. The incident exposed the robust need for Security's involvement in business continuity planning.

- Some CISOs mentioned that the incident caused them to move away from CrowdStrike, while others say it welcomed the opportunity to renegotiate current contracts with the vendor .

> “For some, recovery was smooth as silk. For others, it was a debacle of epic proportions. The number of customers impacted was astronomical. It highlighted the [business continuity] challenge many different organizations and industries face. It is considered one of the largest incidents in outage history. So, we can all learn from this.”
>
> — Mike Restivo, CISO Expert Exchange Host and Kyndryl's US VP Security and Resiliency Practice

Rationalize risk

- The CISOs discussed varying risks associated with using one primary provider and how that can cause problems with a lack of resilience in the case of a cyber-attack or systems outage. While many large providers have made a "platform play," bundling all the services together on one platform or with one cloud provider can be a double-edged sword. On the one hand, it allows all the data and permissions to be managed more seamlessly and often is less expensive, but on the other hand, it does not leave alternative routes and systems to use the data in case part of the system goes down.

- A leader referred to this as a problem of the large providers being "too big to fail." Another member pointed out that large companies like Microsoft aren't held liable when their systems fail, resulting in lost business for their customer companies.

- One leader pointed out that "diversity is good" regarding different data environments. Their company uses two different EDR systems. However, it can still be problematic when a large vendor, such as Microsoft, issues a patch or an update. Another member shared the view that CrowdStrike lost a lot of goodwill with its client base because CISOs always encourage their teams to do updates in real-time, but this best practice got them during the CrowdStrike incident.

“The CrowdStrike incident led us to do an assessment of where we have a high concentration of vendors. How are others determining the level of risk with which you are comfortable? What determines whether you are vested too much with a vendor?"

— CISO Expert Exchange Member

Business continuity planning

- Top security executives are taking active steps to integrate their cybersecurity measures with their business continuity planning. Several members described how experiences with other cyberthreat incidents caused them to create Business Continuity Plans to keep their operations running smoothly as they deal with breaches or threats behind the scenes.

- CISOs are using various tools and metrics to measure their effectiveness in responding to a security breach or widespread outage. In some cases, companies are working with third-party auditors as part of business continuity planning to carry out tabletop exercises that rehearse the company's response to a cyber incident.

- CISOs are increasingly tasked with managing operational resilience in addition to cybersecurity resilience. Due to corporatewide digital democratization, operations can get compromised through a cyber security threat or other non-malicious outage.

- One member mentioned that while operations have historically been separate from IS and cybersecurity, the two have become intertwined and fall under the CISO's remit. The CrowdStrike outage highlighted how they are inextricably related.

"I'm talking with other CISOs and finding that they are also starting to get these broader resilience remits instead of just disaster recovery or business continuity or crisis management. It's starting to expand into full technology stack resilience. We have found many similarities."

— CISO Expert Exchange Member

Kyndryl, Inc. hosts the CISO Expert Exchange. Please contact Michael Restivo with any questions about Kyndryl or this Exchange.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.