Government CIO

Expert Exchange

Q3 Executive summary
July 25, 2024

kyndryl

Overview

In this Expert Exchange session, 12 CIOs convened to discuss how their companies are preventing and responding to incidents, cyber or otherwise, in the wake of the recent CrowdStrike failure. This included implementing better emergency communications plans with stakeholders. In the latter portion of the discussion, the conversation pivoted to identity management. The agenda was created based on advance interviews with participants.

Hosts

Anita Mikus
Kyndryl, Vice President,
Government and Education

Rajesh Jaluka
Kyndryl, Chief Technology Officer,
Healthcare and Government

Key topics

Reacting to the CrowdStrike Failure

- CIOs are focused on the July 19 CrowdStrike failure and its implications for state agencies. The members shared how their organizations responded to the event, with many on the call directly impacted by the cyber-attack. Many used the incident as an opportunity to review procedures, identify gaps in the system, shore up communications infrastructure, and better prepare for a future attack.

- Because the attack happened on a Friday, many desktop support teams in one state were working remotely from home. The different agencies had to deploy their teams quickly to the onsite computers to restore them individually. This often meant 4,000 desktops or more in several other locations.

- Several members described how they used an "n-1" system, meaning that they had set up their computers for resiliency, whereby if one component goes down, it doesn't take the entire system down. However, the individual state agencies' ability to respond to the event quickly varied from agency to agency.

- Several CIOs observed that communications with different parts of the organization outside of IT and the executive team could help or hamper how quickly systems got back up and running. For example, one state's Department of Transportation (DOT) restored its system very soon because the communications infrastructure was already in place for first responders to respond rapidly to emergencies. Some members have emergency communications plans, but they may or may not follow them when an emergency happens. Others shared that they don't have emergency communications plans but need to create them.

- The leaders emphasized the importance of responding to an attack without interrupting customer service (i.e., when responding to attacks on significant infrastructure components such as the power grid). In most cases, the agencies were able to respond to the CrowdStrike attack and restore their systems.

> “Everything was back online, with no downtime to our customers. But we had that because we had the first responder community. The call came in and all kinds of crazy stuff was happening”
>
> — Kyndryl Government CIO Expert Exchange Member

What can organizations learn following the CrowdStrike global IT outage?

Learn more

Preparing through Tabletop Exercises

- The group discussed tabletop simulation exercises, which are an excellent way to prepare for a cyberattack and communicate effectively with non-technical staff, partners, and other key stakeholders about fending off an attack and restoring all systems. Several members shared that they are working with their insurance companies to set up tabletop exercises, which may provide several different kinds of scenarios.

- CIOs are under a lot of pressure from stakeholders who don’t fully understand what’s involved, so working with them on tabletop exercises can help alleviate some of the pressure because they have a better understanding of how their technical teams are prepared to respond to a threat incident. One leader expressed the opinion that state agencies should implement cyberattack drills, just like the fire drills everyone had in school growing up. These drills help people move past the initial panic to action during an actual attack because the response has been rehearsed.

> “We're planning a tabletop exercise with our cybersecurity steering committee members, and I am concerned about ensuring they get the chance to exercise their role. They first asked for a copy of the incident response plan, which is 90 pages of technical stuff ."
>
> - Kyndryl Government CIO Expert Exchange Member

For more information about taking an orchestrated resilience approach

Visit here

Identity Management: Balancing Privacy with Need for Identification

- An ongoing concern for state agency CIOs is how they are balancing the need for user and customer privacy with ease of use for identification. One of the members noted that the "friction" of identity proofing while protecting against fraud remains central to their efforts to digitize all user records. They have adopted a "step-up" identity process where they ask for more information depending on the type of transaction so that more involved transactions require more excellent authentication.

- With some agencies still facing low adoption of digital services (for example, one member's agency offers 97% of its services online, but only 30% of customers use them), ease of use remains a top priority. However, making digital services more accessible while maintaining robust data privacy is challenging.

- States are looking to the Transportation Safety Administration (TSA) as an example of how this balance is done well across different systems, customers, and departments. One state is working on implementing a single-user ID across agencies and noted the importance of including the DMV in the process since the DMV plays a central role in issuing identification in the form of driver's licenses.

"We started online services years ago. We saw fraud in those services, and we made improvements. Some improvements included balancing the friction among identity proofing, the convenience to the customer, and the fraud that would result from that convenience."

- Kyndryl Government CIO Expert Exchange Member

How Digital IDs are Driving Better Experiences

Learn more

Kyndryl, Inc. hosts the Expert Exchange. Please get in touch with Anita Mikus 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.