CISO Cross Industry

Expert Exchange

Q1 Executive Summary
January 10, 2023

kyndryl™

Table of Contents

Host

Mike Restivo – US Sales Vice President – Security and Resiliency

Matthew Rice – Practice Lead, Resiliency Consulting Services

Overview

In this Expert Exchange session, several CISOs convened to discuss the following topics. The agenda was determined based on mutual interest, determined through advance interviews with participants.

Managing resiliency internally and externally

- With the rise of SaaS-based solutions and a greater dependency on the cloud, many organizations no longer have full control over their resiliency. As a result, organizations are having to balance traditional recovery approaches for enterprise critical applications with expectations that vendors should be providing adequate resiliency. Having confidence in vendors' efforts requires holding them accountable to contractual obligations and performing more comprehensive vendor assessments.

- Many vendors, especially the large cloud providers, are unlikely to "flex" for organizations that ask for changes in resiliency measures. Being too dependent on a single provider, especially vendors who refuse to meet resiliency expectations, can pose significant risks to an organization. Mitigating this risk involves having multiple backup plans in case vendors must be dropped for not meeting resiliency standards or if a solution becomes unavailable.

- Continuity planning needs to be an ongoing exercise to ensure organizations don't get caught flat-footed. Too often, organizations carry out what is essentially unit testing rather than integrated testing (e.g., testing recovery for a cloud environment but not testing how that impacts the legacy environment or other clouds). Robust governance around testing, backups, and continuity planning ensures that necessary resiliency steps are being taken.

As you plan in your operational resiliency level and your cyber resiliency, think of it like the King of England—you have the heir, and you have the spare. You may have to have some capabilities that if one solution isn't working, you can flip to another."

— Member, CISO Expert Exchange

A game plan for Cyber Resilience

Learn more →

Cyber recovery: Backing up the backups

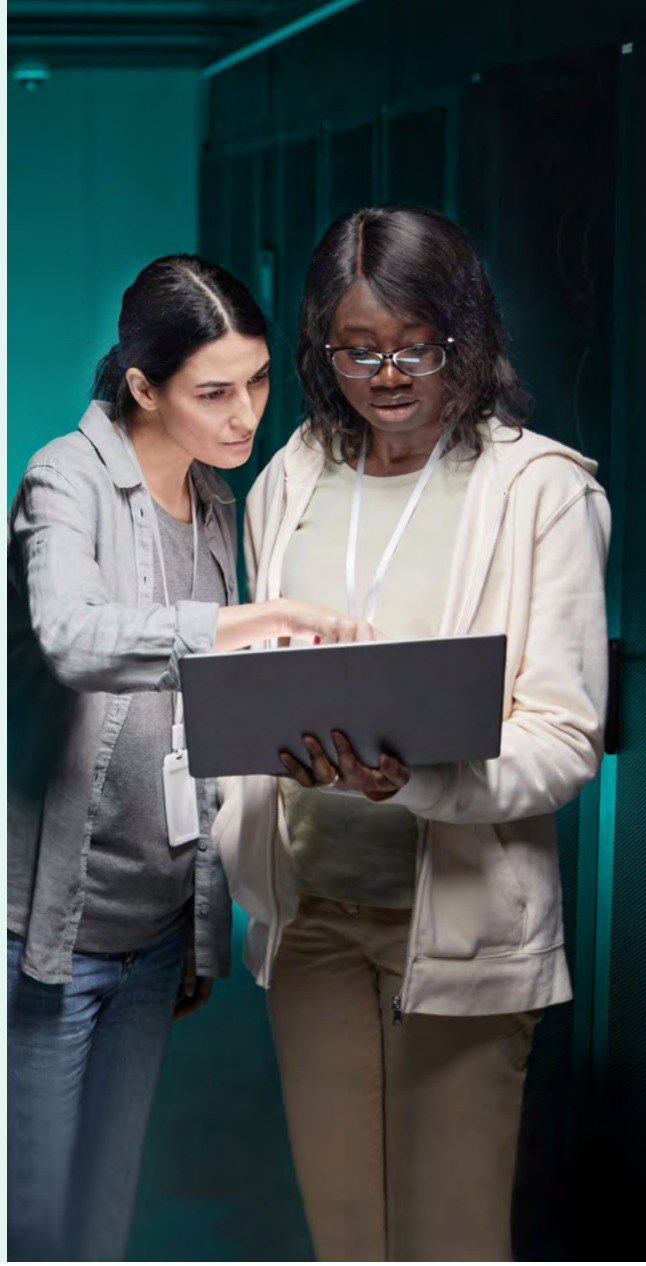
- Cyber recovery does not mean disaster recovery, nor does it mean resiliency—it means that a plan exists with backup copies somewhere that will allow an organization to reconstitute the system. Having backups stored off-site, encrypted in some immutable format gives an organization a head start in recovery in the event of a cyber incident.
- Simply having backups is not enough, as backups and recovery scenarios also need to be tested regularly. A hardware failure or data integrity impact can render DR strategies like real-time off-site replication useless, so having at least historical data that can serve as a springboard for the business continuity plan is crucial.
- Recovery is made more complicated when it in involves multiple points. Recovering from different points (e.g., some recovery coming from immutable vaults, some coming from replicated data) can lead to consistency issues, which underscores the need to test a variety of backup scenarios.

"To the people that are relying on real-time replication in this world of ransomware, where something that gets encrypted is simply going to be replicated across to near real time, I think it's an absolute requirement to have another snapshot out there, sitting separately. It's expensive, but I think that's almost a requirement in today's world."

— Member, CISO Expert Exchange

Two priorities for the CISO

Learn more →



Evolving approaches to cyber insurance

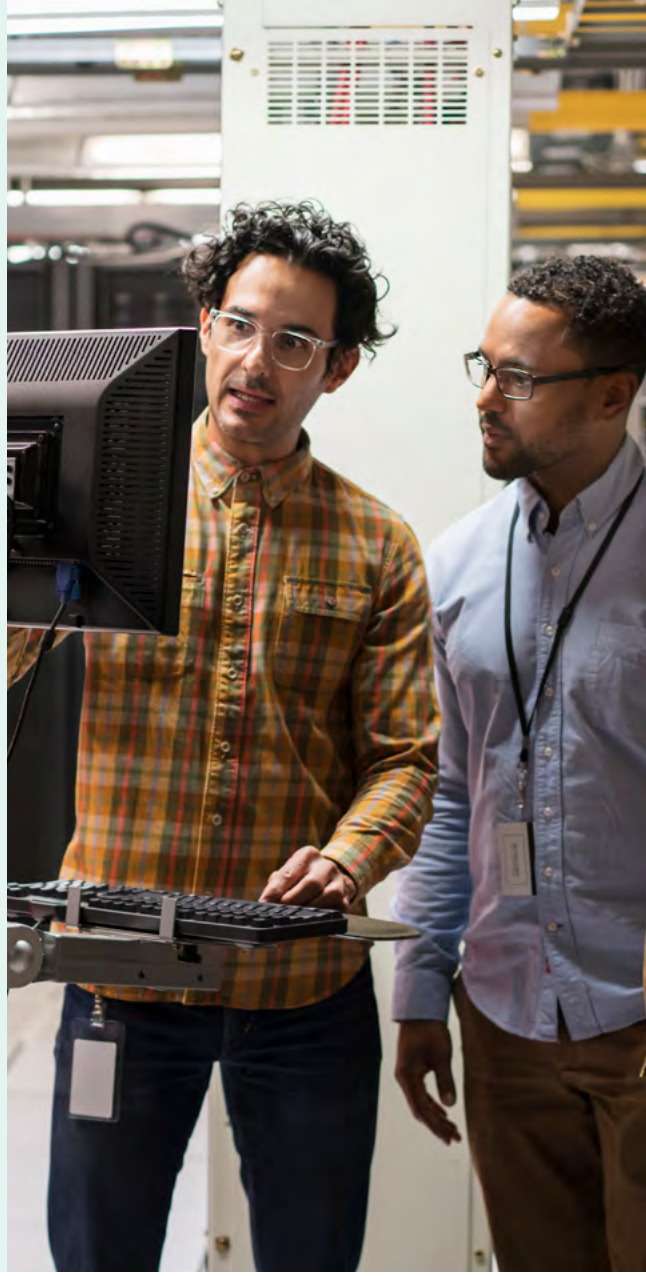
- When marketing digital solutions, it is critical to consider digital equity and the digital equity divide. Government CIOs must consider connectivity and broadband access when strategizing digital solutions, and then presenting those solutions to citizens. Other key considerations include clarifying what services are associated with what agency and how the government is protecting citizen data while they leverage these services.

- There is little to no marketing support behind the roll out of digital solutions, so CIOs must be creative when it comes to marketing. One solution was to cross-pollinate marketing efforts across agencies; for example, the motor vehicle agency website can promote an app being rolled out for an environmental agency.

"We have to be better marketers around how we capture the plans and the dollars that are out there for our citizens and help them understand the direction they should be using it."

— Member, CISO Expert Exchange

The Expert Exchange is hosted by Kyndryl, Inc. Please contact Mike Restivo or Matthew Rice with any questions about Kyndryl or this Expert Exchange.



03-02-2023