Making Cyber Resilience Part of Your Disaster Recovery Plan

Most agencies have a playbook to restore IT systems after a natural disaster, structure fire or power outage.

But government disaster recovery plans should also account for the unique challenges posed by cyberattacks. Agencies should expand their definition of disaster resilience (DR) to include cyber resilience (CR):

- DR has a limited scope and primarily focuses on restoring operations after a single disaster like a flood or hardware crash.
- CR requires a wider scope because a malicious attack can strike multiple targets — including backups — and require more recovery time.

Government Cyber Resilience Challenges

Cyberattacks are dynamic, striking in unexpected ways that conventional DR frameworks don't address.

"A cyber incident may span various applications and locations," says Kevin Chin, cybersecurity technical specialist manager with Microsoft State and Local Government.[1] A ransomware attack, for instance, might compromise backups and the servers set aside to restore data and applications.

Legacy technologies such as mainframes and on-premises systems complicate CR for state and local governments. "A lot of our peers are not upgrading their systems," says Chin, who, as recently as two years ago, has seen systems running software from 2003.

It isn't just technologies that are prone to breaches or attacks. "One of the most compelling issues facing organizations today is the insider threat," says Len Guddemi, director of public sector cyber resiliency at Kyndryl, a global IT infrastructure services provider. Agency leaders don't like to think their own people will endanger public data, but it can happen.

The worst time to analyze disaster recovery flaws is during a ransomware attack. The best time is ASAP.

How to Build Cyber Resilience

With conventional DR programs, leaders create objectives for the maximum amount of data they feel they can afford to lose and the maximum amount of time they can afford to have systems down.

CR requires an updated approach. Cyberattacks are so unpredictable that it's difficult to establish realistic recovery objectives. And protecting your entire estate from a cyberattack is often too expensive. Here are some CR best practices:

Establish priorities. Guddemi recommends a framework inspired by Agile methodologies to help agencies prioritize what to recover in a cyberattack.

First, determine what your agency requires to stay in business. Once you identify the most vital business processes, map those processes to applications and their dependencies, and apply that mapping across their core infrastructure, Guddemi says. Under this framework, make sure there's a clean room or isolated recovery environment to defend against compromised backups.

"If you identify those minimal viable applications in your compute environment and infrastructure, you're going to be able

10-Point Checklist for Modernizing Legacy Systems

- [ ] **Inventory current databases, applications, systems and technologies.**
- [ ] **Align modernization to agency strategies and objectives.**
- [ ] **Assess legacy security risks.**
- [ ] **Perform cost/benefit analysis.**
- [ ] **Choose modern technology, aligning with agency goals.**
- [ ] **Engage end users and stakeholders.**
- [ ] **Implement a robust change-management strategy.**
- [ ] **Test the recovery environment rigorously.**
- [ ] **Adopt continuous monitoring.**
- [ ] **Stay current with industry standards and compliance rules.**

to recover a lot more efficiently and faster in a cyber event," Guddemi says.

Move to Zero Trust. A Zero-Trust architecture improves an organization's mean time to response and mean time to recovery in the wake of a cyberattack. Pillars of Zero Trust include identity access management, multifactor authentication, threat intelligence, data encryption, and identifying third-party and supply chain vulnerabilities.

Follow the data. Analytics, data science and learning automation are essential to CR because they accelerate time to insight. Chin says predictive modeling can quickly identify potential vulnerabilities that manual processes would miss. This leads to fact-based recommendations to show leaders where they need to invest in cyber defense. Moreover, data analytics helps IT leaders remove emotion from decision-making and avoid spending money on ineffective projects.

"I'm in a budget mindset these days," Chin says. "Anything that can help me show leadership where to spend money is better for me."

Test the framework. Agency leaders need business-continuity experience across the full spectrum of incident response, recovery planning and testing. For instance, tabletop exercises that anticipate 15 minutes of downtime in a disaster must be updated to account for the unpredictability of cyberattacks.

"In a cyber event, that recovery could be multiple days," Guddemi says. "You don't know how large the impact zone is." Make sure your training and awareness programs include these kinds of nuances.

Find the right partners. Finally, agencies need partners that can help devise and enforce a robust CR framework. Align with private sector companies that understand your agency's needs and resources.

Analytics, data science and learning automation are essential to cyber resilience.

5 Questions to Ask When Building Resilience

- Are you following established cybersecurity frameworks and how often do you conduct assessments?
- Do you have up-to-date access controls that are aligned with industry-leading best practices?
- Are you encrypting sensitive data?
- Do you have a plan for security management integrated into your development life cycle?
- Do you have a well-defined incident response plan that has recently been tested?

[1] https://webinars.govtech.com/Building-Resilient-IT-Infrastructure--142065.html

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Kyndryl and Microsoft.

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.
www.centerdigitalgov.com.

Sponsored by: kyndryl Microsoft

Why Kyndryl?

Kyndryl has deep expertise in designing, running, and managing the most modern, complex, reliable, and mission-critical infrastructure that the world depends on every day. We are deeply committed to advancing the critical infrastructure that powers progress. We're building on our foundation of excellence by creating systems in new ways: bringing in the right partners at the right time, investing in our business, and working side by side with our public and private sector clients to unlock their full potential.

For more information:

Find out more about the Kyndryl and Microsoft Alliance and how Kyndryl and Microsoft work together around the world. To learn more about how Kyndryl can help your organization achieve its goals, call your Kyndryl representative or visit **kyndryl.com**.

ADOBESTOCK