



How to Become Cyber Resilient

While disaster recovery is important, it's not enough on its own. What organizations need is true cyber resilience: the ability to bounce back from any type of cyber event — from malicious attacks to network outages — without missing a beat. Here are some key points to consider:

- Cyber resilience encompasses not just IT systems, but the end users and business processes that are key to meeting mission.
- A robust solution will respond to any event, whether a cyber incursion, hardware failure, configuration error or network disruption.
- Scalable and automated solutions are vital to delivering continuity of operations.

Government agencies can adopt a new vision of resilience. They can leverage a modernized backup and recovery solution to ensure they are able to meet their mission goals even in the face of rising cyber challenges.



COHESITY



CHALLENGE: Meeting Mission in the Face of Adversity

While federal agencies may be primed to tackle disaster recovery, a number of factors come together to make true cyber resilience challenging.

- **Complexity** can stymie cyber resilience. In heterogeneous IT environments that have evolved over multiple years, it's difficult to deploy protections consistently. Cloud helps with consistent and scalable infrastructure services. However, it also has a learning curve and requires an understanding of the shared responsibility model.
- **Scale** is problematic for on-premises systems. It's typical for an agency to lean on backup systems and even redundant data centers to ensure business continuity. That's expensive, and it adds to the already heavy burden on IT administrators.
- **Automation** can help support resilience, but federal agencies have typically turned to artificial intelligence (AI) and machine learning (ML) as an afterthought, an add-on to systems already in place. To be truly effective, AI- and ML-driven automation needs to be integrated into the resiliency solution from the ground up.

"The machine learning piece needs to be built in from the very beginning, not just bolted on after the fact."

— Ron Nixon, Cohesity Federal CTO and CISO

SOLUTION: The Ability to Recover at Speed

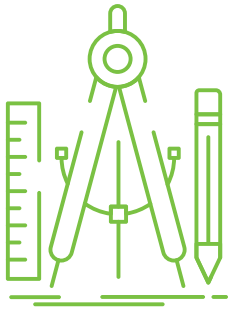
A modernized approach enables agencies to recover at speed from cyber events. It empowers them to not just keep systems running but to effectively support the business processes at the heart of the federal mission. A robust solution will:

- **Address complexity:** A modernized approach offers a single pane of glass, delivering visibility across the IT ecosystem. This helps address complexity by delivering clarity across a wide range of systems and applications in multiple locations.
- **Deliver scalability:** Resilience requires on-demand resources in a cloud environment. This ensures high data availability and rapid recovery while keeping costs even in the face of catastrophic events like natural disasters or cyber events.
- **Integrate automation:** A timely response requires fully integrated automation based on AI and ML. Application programming interfaces (API) enable different pieces of software to communicate via shared definitions and protocols. Thus, an API-driven environment will enable seamless integration of automation tools with diverse security solutions.

"You need a single pane of glass to understand what you're currently protecting, and what you're capable of recovering."

— Sean Phuphanich, Senior Solutions Architect, Amazon Web Services

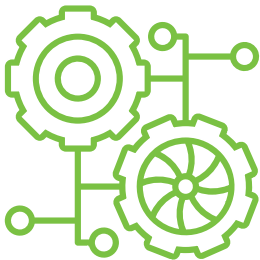
Best Practices in Cyber Resilience



Build for flexibility and scalability.

Cyber resilience requires flexibility and scalability. “In the security realm, it’s a constant game of cat and mouse. So you don’t want to pin the integrity of your entire organization on the chance of someone making a small human mistake or being late on patching something,” Phuphanich said.

Cloud offers scalability, while immutable storage delivers security and simplicity. As threats evolve and new vulnerabilities emerge, “that shouldn’t compromise and invalidate the resilience solution that you have built,” he said. “With a pool of immutable storage, something that is isolated from the rest of your organization, you can have the confidence that data is going to be safe, regardless of what else may happen.”



Integrate systems.

Resilience requires fluidity. “To have resilient systems-and-services organization, you have to be able to pass information up and down within the environment,” Nixon said. This, in turn, demands an approach to resilience that leverages APIs in support of easy integration.

“You’ve got to integrate with the security event management tools. You want to be integrated with the ticketing platform, and the IT service management platforms as well. The data security platform has to be able to inform — and be informed by — the greater architecture as a whole,” Nixon said.



Do operational testing.

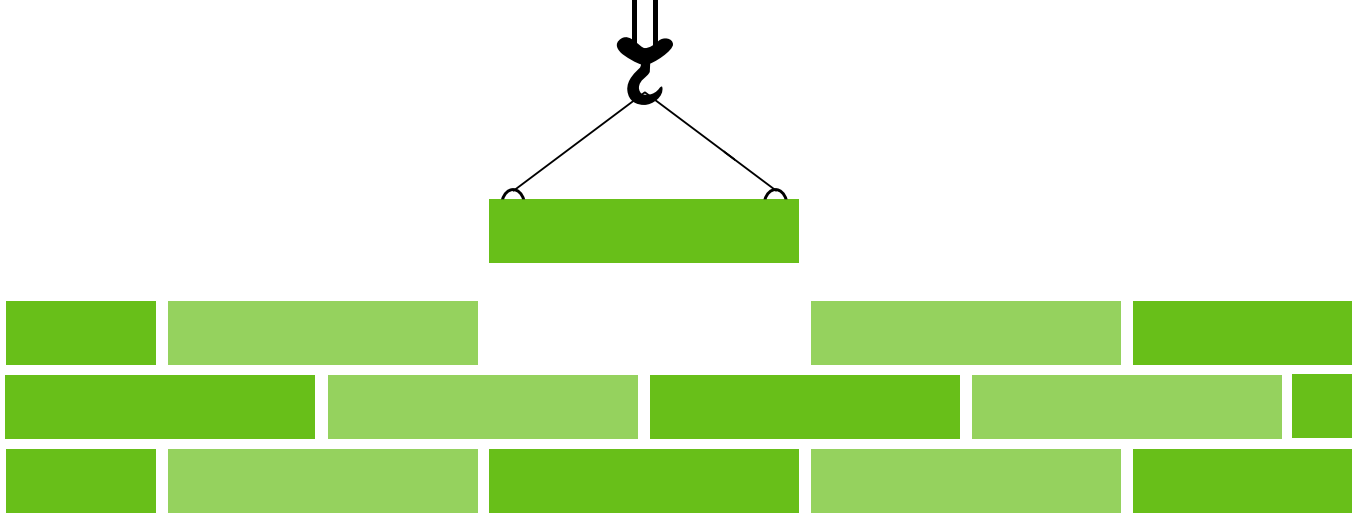
Don’t wait for a crisis to put your strategy to the test. “To be resilient, you have to certify that you’re resilient. You have to test it operationally, as close to real life as you can,” Nixon said. Cloud’s on-demand resources allow you to create and terminate test environments easily and economically.



Take a holistic approach.

Too often, resilience, security and operational responsibilities reside with different teams. But it’s all one mission, and true resilience demands a whole-of-organization approach.

“When data protection and resilience become part of the security strategy and cyber-defense efforts instead of being treated separately,” Phuphanich said. “You unlock the budget and focus of talent that is needed to make your organization more resilient.”



Case Study: Immutable Storage Changes the Game

In the case of one federal agency, a platform approach to resilience helped close a cyber gap.

- **The challenge:** The agency had its data locked in storage, but bad actors were able to change the time settings, accelerating the unlock schedule and making the data susceptible.
- **The solution:** The agency implemented Cohesity's FortKnox solution in AWS in order to improve cyber resiliency with an immutable copy of data in a Cohesity-managed cloud vault via a virtual air gap. By placing the backups outside the normal architecture space, this approach effectively walled off the data from possible malicious exploits.
- **The outcomes:** With Cohesity's Multi-Cluster Manager, the agency achieved immutable storage in the cloud. Strong policies ensured the agency was able to minimize its attack surface, while also delivering a simpler and more consistent implementation.

"With Cohesity and Amazon's S3 Object Lock, they have a high level of confidence, knowing their backups cannot be compromised."

— Ron Nixon, Cohesity Federal CTO and CISO

How Cohesity Helps

Deployed across 200 government agencies, Cohesity supports resilience with products like DataProtect, a backup and recovery solution that eliminates legacy infrastructure silos while reducing costs. Cohesity Helios provides controls to manage user accounts and access in accordance with strong security standards, while SpanFS consolidates data silos across locations by exposing industry-standard protocols on a single platform.

To learn more, visit <https://www.cohesity.com/products/dataprotect/>



COHESITY

