A **GOVERNMENT TECHNOLOGY** THOUGHT LEADERSHIP PAPER | COHESITY AND AWS

5 Keys to Cyber Resilience in Government

Simplify data backup and recovery with the cloud.

As cybercriminals become more sophisticated and focused, data backup and recovery remains an important investment for state and local governments. According to national 2022 data from the Center for Digital Government (CDG), 72% of states planned to upgrade their backup and recovery technology in 12 to 18 months, while 49% of cities and 44% of counties planned to do the same.

Backup data and infrastructure are key targets for ransomware attacks.[1] The number of local governments impacted by ransomware increased from 77 in 2021 to more than 100 in 2022.[2] Governments need a comprehensive cyber resilience approach that protects assets, detects risks, supports response operations, and rapidly recovers data to reduce downtime and ensure business continuity.

"So many government systems must be available 24/7," says Deborah Snyder, CDG senior fellow and former chief information security officer for the state of New York. "Organizations need to address outages and recover critical systems services quickly and efficiently. That makes resilience a non-negotiable requirement."

Relying on legacy backup and recovery technology can increase cost and complexity while limiting flexibility and scalability. This reduces overall cyber resiliency. A smarter strategy uses software-as-a-service (SaaS) delivery from a cloud-based architecture.

"Cloud brings a whole new meaning to cyber resilience," says Dale Zabriskie, field chief information security officer with Cohesity, which specializes in data security and management solutions.

The number of local governments impacted by ransomware increased **from 77** in 2021 **to more than 100** in 2022.

This technology can be foundational for a cyber response plan, compliance risk policy, and cyber insurance requirements. Five best practices explain why.

1. Simplify and modernize

Many organizations have improved their backup service-level agreements by moving from tape to disk-based backup and replicating backups offsite to meet their disaster recovery needs. Replicated disk-based backups are faster than tape but are still susceptible to attacks, as they are often on an adjacent network and accessible through the same user or group credentials.

Adding to the complexity, many agencies use multiple backup solutions scattered across departments, data centers, and cloud instances. They also often deal with aging backup storage hardware. Increasing capacity means increased HVAC, rack space, and cabling. Managing these disparate systems is complicated, less secure, and more time-consuming for IT teams.

"I advise agencies to look for an integrated platform approach," Snyder says.

This simplified route pulls all storage-and-recovery operations into a hybrid cloud-based solution that offers protection and recovery services for on-premises and cloud workloads.

Such a solution simplifies and automates data recovery and isolation through cyber vaulting and disaster-recovery-as-a-service (DRaaS), which provides a flexible, secure interface for data oversight and rapid recovery automation.

Simplicity provides tangible benefits for IT departments. For example, IT managers in Santa Monica, California, spent 90% less time on data management[3] after they deployed a cloud-based disaster recovery system with Cohesity and Amazon Web Services (AWS).

2. Scale and accelerate

"Speed of recovery is the one thing that differentiates an organization getting an 'A' in backup and recovery from those that get a failing grade," Snyder says.

Speed and scale must work in unison. For instance, if constituents pay taxes at specific times of the year, you will need to scale up quickly for temporary needs and scale down when those demands recede. A cyber data resilience program built in the cloud provides all the scale you need with services like Amazon's Elastic Compute Cloud (EC2) and Relational Database Service (RDS).

Moreover, you can optimize cloud-centered cyber resilience to suit your precise data management and protection needs, whether you're operating on-premises data centers or in hybrid or multicloud environments. And you can integrate Microsoft M365 workloads and virtual machines.

A central data management hub using cloud-native services can accelerate data recovery in a fraction of the time you might expect.

"We had one client that needed us to restore 2,000 virtual machines," Zabriskie recalls. "Their recovery goal was four days. We did it in 47 minutes."

Cloud-based recovery can also provide rapid failover to backups for services too important to leave offline for extended amounts of time.

3. Detect and respond

Firewalls and endpoint management technologies are mandatory tools, but they can't keep everyone out.

Cloud-based data management provides extra protection for networks, hardware, workloads, and systems. Such tools use machine learning-based anomaly detection and threat scanning so you can respond and remediate quickly. They do this by finding anomalies in your data, unusual user behavior, and other risks. All this activity appears in logs and data feeds that can drive an effective analysis and response.

"You want to take all that data and visualize it, see what's happening, and know where problems are," Zabriskie says.

4. Isolate and protect

Resilience requires isolated backups. One way to make sure you have a clean copy of your data is to create an air gap that fully isolates data from a network and its hardware.

Air-gapped backups are secure because they are not part of your active network. They reside outside of your infrastructure and can't be accessed if your environment is breached. While tape storage creates an excellent air gap, it's costly and impractical for recovering critical data on a tight timeline.

With modern cloud technologies, IT teams can deploy virtual air gaps that isolate like tape backup while delivering speed and flexibility.

Cohesity Fort Knox, a SaaS data isolation and recovery solution, illustrates how this works: High-value data and workload backups are stored in a separate account secured and managed by AWS. Everything is encrypted into immutable copies that cannot be changed without direct human intervention.

"You want controls that give you total confidence that your datasets are untouchable," Zabriskie says.

5. Classify and prioritize

DRaaS platforms allow you to tailor recovery time objectives (RTOs) and recovery point objectives (RPOs) to your agency's specific requirements.

"Classification and prioritization are at the heart of a sound data governance strategy," Snyder says. "You need a comprehensive data inventory to identify the critical systems, understand how they map back to critical business functions, what data sets are required, and the people required for rapid restoration."

If you want to limit downtime in professional licensing or property tax processing, for example, you can configure your DRaaS platform's recovery objectives to do that. If sensitive personal, medical, or financial data requires air-gapped backups, you have that option, too.

Cohesity provides a data classification solution to discover and classify sensitive and critical data with highly accurate machine learning-based scanning. This allows you to understand if sensitive data was potentially compromised and to respond quickly.

Conclusion

A cyber resilience approach should do more than fend off cybercriminals. It should also make your IT team more efficient, ramp up your data management game, and take advantage of cloud-based tools that help you recover your data according to the need and situation.

"In the event of an incident, cyber resilience enables you to be a hero for your organization," Snyder says.

This piece was written and produced by the Government Technology Content Studio, with information and input from Cohesity and AWS.

Endnotes

[1] https://federalnewsnetwork.com/commentary/2023/01/as-ransomware-attacks-evolve-agencies-must-find-innovative-ways-to-backup-data
[2] https://www.emsisoft.com/en/blog/43258/the-state-of-ransomware-in-the-us-report-and-statistics-2022
[3] https://www.cohesity.com/customers/city-of-santa-monica

ADOBESTOCK