Safeguarding the mission:

Cyber resilience as a priority

The number of cyber incidents targeting Federal agencies has risen significantly, with more than 30,000 reported to CISA last year. But a deeper threat lies in undetected breaches – the stealthy intrusions that begin with the compromise of sensitive data – and result in attacks, years in the making, that can hinder the ability of government agencies to deliver on their missions and disrupt essential public services.

Increasingly, these stealthy intrusions are carried out by state-sponsored cyber criminals. Recently, U.S. intelligence agencies warned that cyber actors supported by the People's Republic of China are seeking to pre-position themselves on IT networks for cyberattacks against critical infrastructure, aiming to disrupt essential services in the event of a geopolitical crisis.

These threats are prompting shifts in government cybersecurity priorities. The National Cybersecurity Strategy emphasizes defending critical infrastructure, actively countering state-sponsored attackers, and investing in resilient environments through public and private collaboration.

At its fundamental level, cyber resilience means that even if an adversary attacks or successfully gains access to an agency's environment, its data, applications, and user accounts can still deliver the agency's most critical capabilities and services.

> "U.S. ... agencies have recently observed indications of Volt Typhoon actors maintaining access and footholds within some victim IT environments for at least five years."
>
> — Cybersecurity and Infrastructure Security Agency

Developing a comprehensive cyber resilience strategy

Cyber resilience requires a mindset and strategy shift from breach prevention to breach assumption. This shift doesn't minimize prevention or detection efforts, but it helps agencies prioritize the protection of sensitive data and continuity of essential operations in the face of an attack.

It also aligns with Federal zero trust requirements, which call for agencies to inventory, categorize, and protect data, both at rest and in transit; deploy mechanisms to detect and stop data exfiltration; and implement data lifecycle security practices.

Key steps to build a cyber resiliency strategy include:

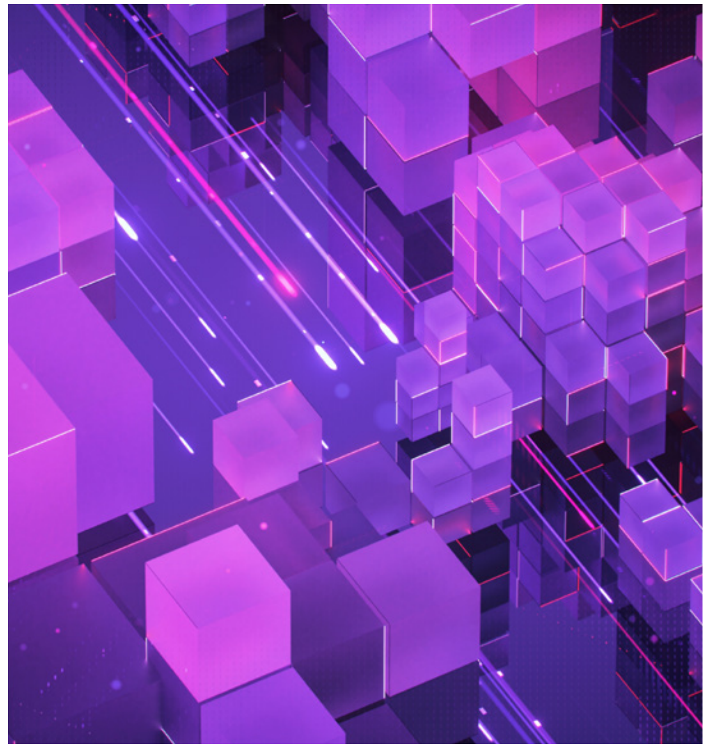
1. **Identifying critical systems:** Determine the most critical systems and services that support the agency's core mission. Prioritize protecting and isolating these mission-critical components, even if it means not being able to protect other systems equally
2. **Implementing safeguards and redundancies:** Build in multiple layers of redundancy and fail-safe mechanisms for critical systems
3. **Prioritizing backup and recovery:** Backups are a prime target for adversaries. Ensure that backup and recovery processes are secure, immutable, and can rapidly restore critical data and systems if they are disrupted or disabled
4. **Fostering cross-functional collaboration:** Conduct regular exercises and testing across IT operations, security, cloud, and backup teams to ensure readiness for major incidents. Develop incident response and recovery plans to quickly restore operations after an attack

A holistic cyber resiliency strategy should achieve four goals: anticipate attacks, withstand breaches, recover from disruptions, and adapt to threats.

Backup and recovery practices drive resilience

Often, backups are a cybersecurity afterthought, but attack patterns demonstrate that they are high-value targets. Ninety-four percent of IT and security leaders experienced significant cyberattacks last year, according to a global survey by Rubrik. Of those, more than 95 percent said their backups were targeted early in the attack lifecycle, and 74 percent could not fully recover.

In a world where breaches are inevitable, the last line of defense is a secure backup and the ability to recover in a secure, trusted state. To accomplish this, agencies need to apply zero trust principles in their data environments overall – and specifically in backup and recovery systems and processes. This means removing implicit trust between system components, so if one component is breached, others are secure, and implementing granular access controls and policies, ensuring only authorized users and processes can access and interact with backup data.



Equipping agencies for cyber resiliency

Agencies need a partner that provides more than baseline compliance with cybersecurity requirements – they need a partner that helps deliver cyber resilience, so agencies can expedite incident response and ensure that mission-critical services continue unabated.

Rubrik collaborates with agencies to develop comprehensive cyber resilience strategies that integrate zero trust principles, navigate the intricacies of cloud environments, and emphasize data backup and recovery, Rubrik Security Cloud – Government and Rubrik Security Cloud – Private help Federal agencies withstand cyberattacks, malicious insiders, and operational disruptions with:

- Air-gapped, immutable, access-controlled backups that can't be modified, deleted, or encrypted by hackers
- Seamless integration with major cloud platforms, enabling organizations to protect and manage data across hybrid and multi-cloud environments
- Improved cyber readiness through testing and policy-driven workflows that ensure fast and predictable recoveries

- Threat containment that ensures safe and quick data recovery by quarantining data infected with malware
- Continuous monitoring for data threats, including ransomware and indicators of compromise, and intelligent risk monitoring to identify and monitor sensitive data exposure

Rubrik Security Cloud – Government has achieved FedRAMP® Moderate authorization. In addition, the platform is built to meet Family Educational Rights and Privacy Act, Criminal Justice Information Services, and Department of Defense Cloud Computing security requirements with:

- A dedicated instance for government agencies and contractors
- Secure processing of government data within the United States
- Always available support by qualified U.S. citizens located on U.S. soil

Navigating the complexities of cloud environments

A cyber-resilient approach can protect agencies' most critical data regardless of where it resides – on premises, hybrid cloud, or multi-cloud. However, as agencies move to take advantage of the flexibility and economies that cloud environments offer, they must also understand the specific resiliency challenges of cloud environments.

The cloud is targeted with more frequency and more success than on-premises environments. It also can be more difficult to defend due to blind spots introduced by object storage and unstructured data. Object storage is typically not machine readable by security appliances; unstructured data may also go unprotected by security technologies and services.

Additionally, the shared responsibility model utilized by many cloud service providers (CSPs) is often misunderstood, leading to security vulnerabilities that are exacerbated in hybrid or multi-cloud environments. Understanding and validating the security responsibilities among CSPs and agency teams is critical to cyber resiliency efforts.

To learn more, visit rubrik.com/federal.

rubrik

MeriTalk