Sled Data Breaches -

Why a cyber resilience strategy is required if agencies want to bounce back from a hack

by Ryan Schradin
Managing Editor

Ever since the beginning of the COVID-19 pandemic, state, local government, and educational institutions (SLED) have found their modernization journeys to be quite paradoxical. Though digital transformation equipped SLED organizations with cutting-edge solutions and next-generation capabilities that deliver tremendous benefits, this technological renaissance inadvertently created a headache for IT teams, as the dissolution of traditional network perimeters opened a door to new challenges and vulnerabilities for IT teams to overcome.

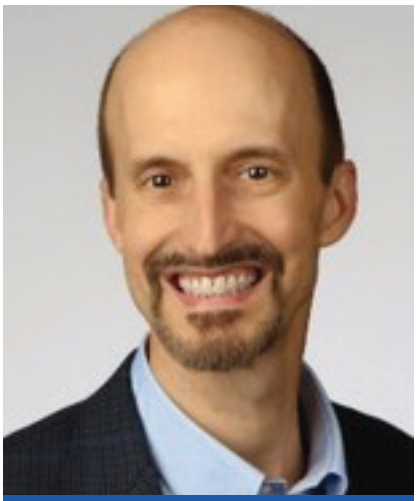
As a result of the pandemic-induced surge in remote technology and cloud solution adoption, networks are more complex than ever. And modernization initiatives have SLED agencies producing more data than they ever have before. And malicious cyber hackers have taken notice, as there has been a considerable rise in cyber attacks against

SLED organizations. To counteract this trend, SLED IT teams are turning their attention to maturing their cybersecurity frameworks to bolster their defenses.

But what happens when an attack does occur? How do SLED agencies begin to respond and recover from a breach or a hack? That is where cybersecurity ends and cyber resilience begins. But what is the difference between cybersecurity and cyber resilience? And what role does cyber resilience exactly play in the recovery and restoration of SLED databases and networks?

To find out the answers to these questions, and to learn more about the current cyber threat landscape SLED agencies face today, as well as the cybersecurity frameworks and solutions that can assist them in protecting and recovering their data, we sat down with NetApp CTO Jim Cosby.

GovDataDownload (GDD): Cybersecurity has been a major topic of focus and conversation in government circles for more than a decade. But we're starting to hear agencies talk more and more about cyber resilience. What is cyber resilience? How is it different from cybersecurity?



JIM COSBY
NetApp CTO

Jim Cosby: Cybersecurity includes the safeguards that an agency puts in place to protect and defend against a cyberattack. Cyber resilience entails the procedures that an agency follows to recover from any attack and get back to normal operations.

Cybersecurity involves things like application security, network security, and security of data in any location like edge, core, cloud, and multi-cloud. Cyber resilience encompasses the abilities an agency should have in place that help them identity, detect, and recover data to restore normal operations, regardless of the attack type or severity.

GDD: We've heard cyber resilience defined as the network's ability to bounce back from an event or continue performing during an event. What kinds of events are we talking about? Is it only cyber attacks, or can other events strain an agency's cyber resilience?

> **"With digital transformation and modernization driving data and application usage to multiple locations from edge to core to cloud and multi-cloud, the cyber risks are amplified."**
>
> Jim Cosby

Jim Cosby: Cyber resilience can include how an agency recovers from an application, network, or data attack. The attacks can involve application and network attacks like DDoS (Denial of Service) attacks where the network and application stop responding to the users due to overloading the network or server with an over-abundance of requests, which halts user access to data.

Malicious cyber actors may also choose to encrypt an agency's data and hold them as a financial hostage, requiring the agency to pay a fee for the return of their data. The data attack can also entail breaches and exposure of sensitive data unless an agency pays a ransom. All these application, network, and data attack events can strain an agency's cyber resilience

capabilities.

GDD: Why is cyber resilience so important today for state, local, and municipal governments? Would you say that digital transformation and modernization initiatives have made it more important in recent years?

Jim Cosby: Cyber resilience capabilities such as identify, detect, and recover are some of the key steps needed to get an agency's mission back up and running again after an attack. If they lose mission function, it could impact government services like power, water, police, and medical care. These are critical for the protection and health of our citizens and country.

> **"These new exposures emphasize the importance of knowing and following data governance and compliance to ensure that data and information are well protected."**
>
> Jim Cosby

And with digital transformation and modernization driving data and application usage to multiple locations from edge to core to cloud and multi-cloud, the cyber risks are amplified. Now it is even more important to have proper cybersecurity and resilience.

GDD: What steps should state, local, and municipal government organizations take if they're looking to start increasing or improving their cyber resilience? Where do they start?

Jim Cosby: SLED agencies should start with the five basic steps of the NIST Cybersecurity Framework. The five steps include identify, protect, detect, respond, and recover. Agencies should develop a set of capabilities around each of these steps, if they want to achieve mature cyber protection and have the ability to successfully recover if attacked.

They should start by educating themselves on the framework, then assessing what they have to protect, and finally develop their strategy from there.

GDD: Has the complexity of today's networks and the introduction of cloud, multi-cloud, and hybrid environments made cyber resilience easier or harder? Why?

Jim Cosby: Network changes like faster speeds and newer topologies have increased data flow and access. Data access in hybrid cloud and multi-cloud environments has increased the amount and number of copies of data in multiple locations, which increases the workload around data governance and compliance.

This new data quantity and availability have exposed more data to many more touch and management points, as well as to many more users and data administrators. These new exposures emphasize the importance of knowing and following data governance and compliance to ensure that data and information are well protected.

GDD: What technologies and solutions can help government agencies increase their cyber resilience?

Jim Cosby: There are many procedures that can help agencies increase cyber resilience, and they revolve around the NIST cybersecurity framework.

First, identify what you have with tools and services like NetApp Cloud Data Sense. Second, protect your data with strong backup and recovery capabilities – as well as encryption of data – at rest and during transit.
NetApp offers Snapshots, which are pointer-based copies of data that provide instantaneous, multiple recovery points for any data in any location. NetApp also has SnapMirror replication capabilities to provide multiple

copies of data from edge to core to cloud and multi-cloud. We also offer Cloud Backup Service which provides a separate distinct backup copy of data to a cost-efficient, intelligent object data target both on-premises and in the cloud, as well as in multi-cloud environments. NetApp's immutable backup technology on-premises and in the cloud can prevent any attacker or devious administrator from corrupting or destroying the backup copy, which provides a guaranteed way to recover data after an attack.

Third, use technology that can detect cyber activities like NetApp ARP (Autonomous Ransomware Protection) to track UBA (User Behavior Analytics) to gauge what is normal and what is an anomaly, which can then trigger an instance SnapShot backup before data access is allowed. This produces a backup copy of the good data before the attacker makes any changes.

Fourth, be able to respond and notify all involved parties and users so they know what actions to take and not take. NetApp has multiple offerings like System Manager, ActiveIQ, and BlueXP IT estate management tools that send notifications of cyber activities using ransomware dashboards and alerting mechanisms. And lastly, make sure your recovery is quick and accurate like using NetApp SnapShots, SnapMirror, and Cloud Backup Service to be able to accurately recover any data anywhere any time.

"Make sure your recovery is quick and accurate like using NetApp SnapShots, SnapMirror, and Cloud Backup Service to be able to accurately recover any data anywhere any time."

Jim Cosby