MeriTalk
Improving the Outcomes of Government IT

COHESITY

In the Federal Fight Against Ransomware Attacks, Holistic Data Protection Plans Include Backups

Cyber threats, including ransomware attacks, are now a national security issue as bad actors target Federal agencies and our nation's critical infrastructure. Protecting Federal agencies against these cyber threats is a national imperative, evidenced by the Biden administration's cybersecurity executive order mandating that agencies take additional measures to secure Federal infrastructure.

MeriTalk recently talked with Steve Grewal, Vice President and CTO, Public Sector at the data management platform provider Cohesity, and former senior executive (CIO/CTO/CISO) for the General Services Administration (GSA), Department of Education (ED), Department of Transportation (DOT), and Health & Human Services (HHS). Grewal spoke to us about Federal cybersecurity risks, the changing role of backup solutions, and how agencies can protect against loss due to a ransomware attack.

MeriTalk: It feels like every time we turn on the news, there is a report of another ransomware attack. Based on your experience at the Education and Transportation departments and GSA, what distinguishes Federal agencies from other ransomware targets? What are their biggest vulnerabilities?

Grewal: The biggest differentiator is the national security assets that the Federal agencies hold. Just looking at the agencies where I worked – people think the Department of Education is a policy making organization, but it is actually one of the largest holders of personally identifiable information. The department houses more than 100 million identities submitted through applications for the Federal student aid program. Looking at the Transportation Department, it oversees operations like air traffic control and other critical infrastructure such as pipelines. Their work highlights why Federal agencies are a prime target – they have critical information that attackers would love to have, and control.

The largest vulnerability, unfortunately, is the underlying technology for a lot of these systems. Some systems are using technology that is over three decades old. If we think about the speed that attackers and adversaries are moving versus the pace that Federal agencies upgrade systems and adopt new technology, there's a significant gap.

MeriTalk: The transition to remote working dramatically expanded the potential cyberattack surface. How well have agencies responded?

Grewal: I think it's been a mixed bag. GSA was very progressive even pre-COVID-19; telework was largely permitted. Other agencies had a very conservative approach to telework. Many Social Security Administration employees didn't even have laptops or mobile devices, and their remote access systems didn't have the capacity for telework.

Agencies took expedient action as a result of COVID to move to telework environments, which caused the attack surface to expand in a big way. Now we're in a scenario where maybe 80 percent of employees are working from home, and attackers can take advantage of that. Some agencies have done a good job of ensuring the proper level of visibility and coverage in the remote environment. With other agencies, it's still a work in progress. Funding helped address those gaps, but we still have a mixed state across the Federal landscape.

MeriTalk: Most agencies operate a mix of legacy and cloud-based IT systems as they continue their modernization journeys. How does this affect their ability to defend against ransomware and other types of cyberattacks?

Grewal: Many enterprise security tools that agencies use have been designed for on-premises assets. Some have been tailored for services like email and collaboration tools, but in large part enterprise security architecture has not been recalibrated for decentralized data and services. Agencies don't always have visibility into how they're consuming services.

I always recommend that agencies map out data flows — and not get so focused on the perimeter, boundaries, or the physical location. Maybe identity management systems initially authenticate inside the data center, but then they interact with applications in Google, Microsoft, and Amazon. If there are interconnections to other environments, having those data flows mapped helps the technology team better understand how to tailor their security architecture.

Agencies really need that holistic view, but they haven't made the required investments. Hence, we have blind spots. Because of poor visibility across the enterprise, some agencies don't detect an attack or adversary inside their environment for over 180 days.

Once they're inside, hackers' lateral movement and leapfrogging result in further damage. The hackers may get in through email phishing and hit one system, but that system connects to another system and that system connects to another system. That's where the dispersed attack surface comes into play. It's also why it takes time to detect that they are even there.

MeriTalk: Hackers are increasingly targeting data backups to infect networks with ransomware and malware. How big is this problem, and why are backups a vulnerability?

Grewal: It's a major problem. In the last 24 months, we have started to see a convergence between backup or data protection and cybersecurity requirements. Historically, backups were just viewed as an insurance policy and attacks were just about destroying them. But now hackers are attacking the backups and encrypting them as a way to get ransom.

Your backups are only as good as your ability to restore them – backups are worthless and restores are priceless. The only effective strategy to protect against ransomware attacks on your backups is a data protection solution that includes security characteristics like immutable backups, policy-based automated air gaps, and a single software-defined platform, allowing you to reduce the attack surface.

MeriTalk: What are some of the things Federal agencies can do to protect their backups?

Grewal: The ability to test processes to ensure that they're able to restore backups is huge. Agencies should perform an assessment to confirm whether backup solutions are tamper proof and that they have strong authentication, data locking, and anomaly detection systems in place.

My advice to agencies that are looking for a refresh or wholesale replacement is to assess vendors based on whether their technical requirements and success criteria have those key things built in to ensure that their backup solutions can sustain a ransomware attack. Also, agencies must always have an original copy of the data and use additional copies to perform other functions.

MeriTalk: As agencies migrate more data and applications to the cloud, how should they think about backups?

Grewal: Their backup and data protection strategy should cover the cloud, on-prem data centers, and the edge. There's a misconception that if you're in the cloud you're taken care of. But cloud providers are all about scale, providing technical offerings in a cookie-cutter fashion that don't always give the granularity and backups you need. Whether you're compromised in the cloud or in your data center, your strategy should give you the ability to return to a known good state.

MeriTalk: How can emerging technologies like machine learning help to defend an agency's data against attacks?

Grewal: We're moving away from traditional signature-based security, which was all about matching certain identifiers. With the massive increase in data volume, machine learning can proactively benchmark user behavior and detect anomalies. Being able to leverage automation to pivot and change is critical for effective cybersecurity.

The goal is to prevent zero-day attacks and evasion techniques. We've done a pretty good job with known threats, but not unknown attacks. Machine learning and artificial intelligence will give us the ability to increase our batting average when it comes to intercepting unknown attacks.

MeriTalk: If an agency does fall victim to an attack, what should it do to minimize the impact to daily operations without paying the ransom?

Grewal: They must test their contingency plans and disaster recovery procedures before an attack. It's not just a paperwork exercise. Regularly simulating incidents, performing failovers, and testing other environments and copies of data will provide the greatest ROI if an agency is compromised. They need another copy of data that is air gapped, meaning a copy of sensitive data is offline, disconnected, and inaccessible from the internet, and not commingled with the environment.
Historically, testing across the Federal landscape is done on a very limited scale and largely as a compliance paperwork drill. If you get hit by a ransomware attack and want to take a firm stance against paying ransom, the only way to do that is by restoring operations. Otherwise, you're in a bind. Agencies can always stand up new compute, servers, connections, and links. That's easy and can be done quickly. It's the data that they'll never get back.

MeriTalk: How can Cohesity help Federal agencies secure backups to protect against ransomware and other malware attacks? What sets Cohesity apart from other enterprise backup and data management providers?

Grewal: Cohesity is a data protection backup vendor that gives you all the defense mechanisms that you need for ransomware – those key attributes that I talked about earlier are baked in; you get those on day one. As agencies are looking for either refreshing or replacing their backup solutions, some things are non-negotiable: immutability, data locking, worm compliance, and air gapping. Our platform provides all those protections so you can quickly and expediently restore to a known good state. More importantly, you proactively have the right protection and defense mechanisms and controls in place.

Over 85-plus percent of our customers start with backup; that's where we started and where we shine. Once you get started with backup, Cohesity can help agencies solve the bigger issue of data management. Think file services, object services, data lakes, disaster recovery – all those areas fall under data management.

Over the past 20 years, a lot of innovation has given agencies options, but the one side effect has been mass data fragmentation, which is a three-part problem. First, there's a proliferation of data and sprawl as people use cloud and or edge solutions.

Second, it's very inefficient and ineffective because you're moving data across environments, providers, and this broader ecosystem – using different technologies. Third, government does an incredible job of capturing information, but it struggles to make that data available for analysis and mission enhancement.

The solution to mass data fragmentation is a platform with a broader data management vision. That's where Cohesity can help. We make backups better, stronger, and cheaper, but then you can continue that journey with us on a broader modernization roadmap, so you have the leanest and most effective data footprint. And you have Cohesity's biggest differentiator: a big-picture view of data. We are the only backup company with the broader vision of tackling mass data fragmentation and providing a scalable, secure platform.

Agencies vary greatly in maturity, size, skillsets, budgets, and readiness, but they need to determine the appropriate delivery model. You can consume Cohesity purely on-prem, via software-as-a-service, at the edge in a field or branch office, or with a managed service provider. We support all those models because we understand government complexity.