The Three Keys to Effective Cybersecurity:

Protect, Backup and Defend

Federal agencies face increasingly skillful and potent cyberthreats from state-sponsored attackers, supply chain infiltration, insidious ransomware, and silent network lurkers, but a trio of actions can protect against those assaults.

The drumbeat of significant cyberattacks got louder and faster between 2020 and 2021, as federal agencies altered their operations to accommodate the new work environment forced by COVID-19. The massive SolarWinds supply chain attack and the Pulse Secure virtual private network exploit that hit federal networks, as well as the ransomware attack on Colonial Pipeline's business infrastructure, all showed cyber criminals were continuing to sharpen their techniques and aim them at government and significant national critical infrastructure.

According to a recent 451 Research Digital Pulse Flash Survey, the pandemic is driving a lasting digital transformation of IT. "Responding to operational challenges posed by 2020 required enterprises to rely on new technologies," the report said, "and 83% of enterprises surveyed describe some degree of transformation in their IT business operations as a result. More than half (59%) of those report being more security-conscious in their decision-making, and almost as many (57%) note increased reliance on cloud-based technologies. Nearly half (48%) also note greater automation in their IT infrastructure operations."

The costs for cyberattacks for government agencies aren't just measured in the dollars to fix them. They include potential breach of secure data, loss of intellectual and personnel data, and extreme remediation costs. For critical infrastructure providers, who have ties to federal agencies such as the Department of Energy and the Department of Homeland Security, the attacks can mean big dollar ransom payments and possibly expensive fines for compliance violations.

The victims of the attacks also face steep reputational damage, as networks are exploited and users have to navigate a shaky post-attack environment.

Quick Pivot to Remote Work

The COVID-19 pandemic forced organizations of all sizes, in the government and industry, to deploy digital transformation strategies, even if they were not fully prepared to do so. Moving millions of employees to work-from-home status and pushing data and applications to a cloud-based

infrastructure without time to fully vet the cloud service providers resulted in organizations prioritizing business continuity over cybersecurity and setting themselves up for data breaches.

For federal agencies that are increasingly relying on cloud services providers, supply chain attacks, like the one attack that hit SolarWinds, have particular resonance.

Part of any supply chain evaluation is to ensure their new providers actually offer the promised security services. At the same time, internal IT teams have to better understand their new, exposed attack surface in light of the vastly expanded number of network-connected endpoint devices and cloud services outside the protections of the corporate firewall.

Federal agencies have to take a new tack in evaluating their cloud providers in light of the pandemic and increasing reliance on cloud, said Steve Grewal, vice president and chief technology officer at Cohesity Public Sector, a provider of business continuity, data backup, disaster recovery and other software and services for cloud and on-premises data centers.

According to Grewal, a combination of three of the five cornerstones of the National Institute of Science and Technology's (NIST) Cybersecurity Framework align with the Cohesity approach to securing data that can be the keys to better cybersecurity in the new and changing security environment. The first two pillars of Cohesity's cybersecurity solution are proactive -- protecting the backup and detecting vulnerabilities. The third pillar, which is reactive, is rapid recovery.

Antiquated Infrastructure

Before the pandemic, many networks relied on tools that were not necessarily intended to work well in a decentralized manner. With the increase in Software-as-a-Service (SaaS) and cloud-based computing, enterprise IT teams often do not have sufficient visibility into their networks. That can mean they might not have the same levels of detection and response capabilities for the decentralized infrastructure that they have for their on-premises infrastructure.

As a result, data breaches, such as the massive ransomware attack on Colonial Pipeline, are possible because of antiquated infrastructures. "If we think about national security and some of the critical infrastructure elements, some of that continues," Grewal said. "Even the pipeline SCADA [supervisory control and data acquisition] systems are very much built around antiquated infrastructure."

Federal agencies have to take a new tack in evaluating their cloud providers in light of the pandemic and increasing reliance on cloud.

—STEVE GREWAL, VP AND CTO, PUBLIC SECTOR, COHESITY

Solving this dilemma requires basic security hygiene tasks that are often ignored. "As we think about the attack surface, you really need to do a mapping of how the data travels, the inter connections," he noted. It is essential to understand the various threats and devices that are IP-enabled and connected to get a better sense of the connectivity and how the data traverses.

Protection includes an immutable backup, data locking, multifactor authentication, encryption and air-gaps. Detection includes machine learning-driven anomaly detection, daily change rate on local data and stored data, plus pattern-based analysis on historical data. The rapid recovery leg includes machine learning-based recommendations, discovering vulnerabilities for a clean recovery and restoring at scale. Cohesity's unique immutable architecture ensures that backup data cannot be encrypted, modified or deleted and incorporates machine learning to provide continuous monitoring for any anomalies in your data.

Not all data is equal, Grewal emphasized. Some data might be the organization's crown jewels, while other data is not as critical, such as public-facing material that also exists on the freely accessible public-facing federal agency websites. Classifying, categorizing and tagging data by priority can help better segment and isolate the most valuable data. It also helps to understand exactly where data resides and how secure it is.

"First and foremost, you need to ensure that you have a global anomaly tracking approach. You really need a holistic view into your environment," Grewal emphasized. The greater amounts of data an agency has, the more behavioral baselining it should do, he said. Having that view into the randomness of data, and how that changes over time, is essential to understanding and managing the data.

Grewal said IT teams need to monitor file system changes that take place in the environment, so any files that are added or deleted, modified or unmodified, are incredibly important. Having granular logging and auditing for all of those changes in your data, no matter where that data lives, are key components to providing that holistic approach to security he suggested.

These changes can take place at the edge, a branch or field site, a data center that could be in the cloud or in a colocation environment. "You need those areas to be tracked and managed across that entire fabric of your data

assets, in addition to managing your identity component," he said.

Proactive Business Process Continuity

Positioning security teams to respond quickly and efficiently to a malware or ransomware attack requires more than simply having an excess of tools available, even if some are considered "best of breed," according to Grewal. Blindly investing in tools that might not work seamlessly together is a recipe for disaster, not a solution to the malware problem. No matter how efficient a tool might be on its own, if it cannot work within an agency's security environment, it detracts from the overall effectiveness. It does not enhance it. Being purely reactive to breaches and hoping your tools will solve the problem puts network operators at a significant disadvantage when an incident occurs.

"I think it's a culture shift, a technology paradigm shift," said Grewal. "You need a data-first mindset."

Proactive cybersecurity is far more popular in the European Union than it is in North America, which tends to focus on the reactive components of recover and restore from the NIST Cybersecurity Framework, according to Grewal. He attributes this in part to geopolitical biases that date back decades, but added that the Biden Administration's executive order on improving the nation's cybersecurity could help swing the pendulum to a more proactive stance in the United States.

Proactive defenses, such as building a zero-trust architecture that combines active threat intelligence, reducing the attack surface, a zero-trust security framework and active backups that are immutable with data-locking capability and isolation can go a long way to providing a fast restore of compromised servers, whether they are on premises or in the cloud.

Real-life Example

Healthcare facilities, from small clinics to vast health care networks operated by federal agencies and commercial providers are high on the list of ransomware targets in part because they provide critical care and rely on up-to-date information from patient records. They have to remain up-and-running or face significant consequences in patient care. Security experts say, however, that a high percentage of medical center personnel are trained mainly in medicine, not cyber security. Medical insurance data and credentials are highly sought on the dark web because they are valuable commodities to financially focused criminals.

For those who question how a reliable backup can make a difference during a cyberattack, they need only look to Sky Lakes Medical Center in Klamath Falls, Oregon. Sky Lakes Medical Center prepared for a possible ransomware attack by upgrading its data center infrastructure to Cisco HyperFlex, a hyper-converged compute, storage, and networking system, to reduce the costs and operational expenses. It also set up Cohesity to manage backup and unstructured data while continuing to use Cisco HyperFlex for primary (latency-sensitive) data. Sky Lakes saw tremendous value in the Cohesity multicloud data platform because it supports multiple data services. In addition to modern backup, Sky Lakes relies on Cohesity SmartFiles, a software-defined solution for file and object services that goes beyond traditional scale-out NAS within the same cluster.

When cybercriminals hit the medical center's network with ransomware, the security team was prepared and recovered control in minutes. "If we had not teamed up with CDW to learn about the Cisco-Cohesity solution, and had still been using our legacy product and had to go back to tape, it would have taken us weeks, not minutes, to recover. And because we only save 90 days, we would have lost roughly three months of data. With CDW, Cohesity and Cisco, we lost nothing," said Nick Fossen, manager of technology solutions at Sky Lakes.

Looking ahead, taking a proactive stance against cyberattacks in general and ransomware in particular will not only reduce an organization's cyber vulnerabilities, but potentially it can reduce risk-related expenditures.

Learn more and determine how vulnerable your organization is to a ransomware attack with a free assessment at www.cohesity.com/fedsecurity

Traditional storage snapshot technology is only the starting point. It does not ensure that the backups are free from reestablishing the ransomware threat when restoring the image. A truism amongst IT continuity experts is that backups themselves are worthless; restoring a backup is priceless. Clarifying that idiom, successfully restoring an infected backup that reintroduces the cyberattack also is worthless. Restoring a backup purged of malware threats that contains all of an entity's data to get it running at full capacity while updating security patches is priceless. That is an example of data resiliency.

The concept of building an immutable and protected backup that eliminates vulnerabilities is a huge step forward from the simple snapshot technology of 20 years ago. Cohesity, in partnership with Tenable Inc., a vulnerability management platform provider, is leveraging the Tenable.io engine and the common vulnerabilities and exposure (CVE) database's actionable recommendations to ensure that backups are up to date when they are restored and brought back online.

"We've developed a capability where we can scan the backup in an offline fashion and what's backed up in that backup. So whether it's a VM or container, [we can] check the level of patching and vulnerability and bring it up to date in an offline fashion before we actually introduce it to the production network and bring it back online," noted Grewal.

Predictable Backups

In a February 2020 ESG Research Report titled The Evolution from Data Backup to Data Intelligence, barely half of the respondents said they were making progress addressing data silos as a problem impacting IT budgets and strategies. Organizations understand they have backup issues, but when only 52% say they are "making progress" and just 35% say they classify all of their data, the problem comes sharply into focus: Data is clearly at risk.

Without knowing what data an organization has, where it is located, and where it sits in terms of priority for business process continuity, the group can end up spending a lot of time and money protecting the wrong data at the wrong time with the wrong protections. According to the ESG report, "A chasm exists between traditional 'dumb' data backups, in which data is only moved around, but not leveraged to drive or support business outcomes, and data management, in which data is better understood and reused for other technical or business purposes. The data protection space is undergoing a fundamental shift from traditional backup and recovery with the emergence of more autonomous AI-based solutions."

> **"First and foremost, you really need to ensure that you have a global anomaly tracking approach. You really need a holistic view into your environment."**
>
> **— STEVE GREWAL, VP AND CTO, PUBLIC SECTOR, COHESITY**

Grewal said that enterprises "have to be focused on the behavioral aspects of identifying threats. In our case, and more broadly in industry, when we think about detection, it's not just the matching that uses [malware and virus] signatures. It's leveraging AI (artificial intelligence) and ML (machine learning) to get a better sense of anomaly detection and a better sense of those behavioral characteristics that we see that don't align with what we think is normal.

While AI and ML are not silver-bullet solutions, he said, organizations must be aware of the volume of data and the volume of threats in the ever-shifting landscape of cybersecurity.

"First and foremost, you really need to ensure that you have a global anomaly tracking approach," he said. "You really need a holistic view into your environment." Cohesity's solution, for example, provides a single, easy-to-manage software-defined network. Enterprises potentially are dealing with a highly geographically dispersed data footprint with multiple service providers and cloud providers, along with its own internal managed assets and environments.

These enterprises need to identify the time series of data stream so that the sequence of data, timing of data, how data is read, when data is read, and when data is written is clearly understood. This ensures a complete view into the time series of those data streams. This is "absolutely critical in the event that you are dealing with a potential anomalous activity," he added.

Learn more and determine how vulnerable your organization is to a ransomware attack with a free assessment at www.cohesity.com/fedsecurity