DELL EMC intel

CYBERSECURITY MODERNIZATION

How Agencies Can Transform Government While Controlling Business Risk

GETTYIMAGES.COM

Security and risk management is the top priority for state CIOs in 2018.[1] As state and local governments transform their IT environment and workforce, they're finding that the right security approach is critical to their success. Moving systems to the cloud, introducing mobile devices into the workforce, investing in smart city projects and undergoing other modernization efforts can introduce risk if agencies can't sufficiently protect their data. According to a recent survey, 92 percent of government respondents will use sensitive data in an advanced technology within the year, yet 96 percent consider themselves "vulnerable."[2]

While CIOs and other leaders recognize the importance of security to reduce risk and streamline operations, state and local agencies often operate ineffective or obsolete solutions. To combat increasingly sophisticated cyberattacks and protect data and resources, agencies need to transform security. Transformational security moves an organization from a reactive, restrictive approach that hinders modernization to one that's resilient, adaptable and agile.

TODAY'S GOVERNMENT CISO SLEEPS WITH ONE EYE OPEN

The ever-expanding demand for government services, workforce shortages, uncertain funding and other challenges give important nuance to security discussions. IT leaders are under pressure to:

Manage and protect the extended organization. Today's government IT organization is increasingly borderless, with processes and services being consolidated, offloaded or shared across multiple internal and external resources. Besides the traditional on-premises data center, agencies rely on cloud-based services, shared services, mobile devices, the Internet of Things (IoT) and other technologies to conduct business, manage resources and provide services. In addition, agencies are high-volume data aggregators, maintaining financial, health and other sensitive personally identifiable information for citizens, employees and the private sector.

- **Cloud-based services –** In the Center for Digital Government's recent Digital Cities Survey, 93 percent of responding cities had up to 40

SHUTTERSTOCK.COM

percent of their applications and systems in the cloud. One growing cloud-related challenge is the use of unsanctioned cloud apps (i.e., shadow IT). In a recent analysis, most CIOs thought their organization was using 30 or 40 cloud apps; the actual number was an average of 928. The analysis also found 25 percent of data used in shadow IT is shared internally, externally or with the public. Of particular concern was that 3 percent of that data contained personally identifiable information, payment card information, protected health information or other data that falls under regulatory compliance.[3]

- **Mobile devices –** Many government organizations allow employees to use mobile devices and applications to improve productivity and engagement. These organizations must protect data and ensure workers comply with internal, local, state and federal regulations related to data storage and sharing — regardless of the device type, carrier or owner. In a Ponemon survey of IT and security professionals, 67 percent said "it was certain or likely that their organization had a data breach as a result of employees using their mobile devices to access their company's sensitive and confidential information."[4]

- **The Internet of Things (IoT) –** Public agencies are increasingly incorporating IoT devices, sensors and cameras into law enforcement, asset management, smart city projects and critical infrastructure. These solutions allow states and cities to be more innovative and operate more efficiently; however, they also introduce risk. To take full advantage of them, security leaders need to monitor endpoints and implement other security controls to ensure data and critical systems are properly protected.

Securely accommodate citizen demands for digital government. More than 70 percent of U.S. citizens in a recent survey said they expect interactions with their state government websites to have the same standards for quality and security as their private sector counterparts.[5] Organizations can meet this demand, improve the work environment and achieve other benefits by offering secure digital services for sensitive transactions. With appropriate controls, citizens can conveniently pay parking fines, file taxes, submit health information and complete other tasks via their mobile devices or web browsers. The challenge is to provide strong encryption, identity management, access control and other security measures — while also ensuring these measures do not degrade the user experience.

In 2017, approximately 350,000 cybersecurity positions went unfilled in the United States, and recent predictions for cybersecurity workforce shortages globally range from 1.5 million to 2 million workers by 2019.

Address the shortage of qualified security professionals. In 2017, approximately 350,000 cybersecurity positions went unfilled in the United States, and recent predictions for cybersecurity workforce shortages globally range from 1.5 million to 2 million workers by 2019.[6] These shortages will likely impact public sector organizations more severely due to competition with the private sector's salaries and benefits. To mitigate these challenges, organizations need a systematic security approach that includes automation, context-specific incident response and other practices that optimize the use of each cybersecurity worker's time and skill level. In addition, they'll need to implement innovative retention strategies.

"Right now, the top thing on people's minds is staffing and keeping the best talent. It takes time to build camaraderie and team work. You don't want to lose that momentum," says Dan Lohrmann, the former Michigan CISO and current chief security officer for Security Mentor, a national security training firm that works with states.[7]

Improve workforce security awareness. In a poll of local government IT officials, a majority of respondents said their biggest concern was lack of security awareness by workers and end users.[8] Rightly so. In an analysis of cybersecurity attacks, one report found human error was a contributing factor in more than 95 percent of incidents.[9]

It's critical state and local governments ensure employees have basic security awareness

and training to combat some of the most common threats and vulnerabilities. These threats include social engineering (e.g., phishing attempts), weak or exposed passwords, use of public WiFi, shadow IT, security workarounds on mobile devices and more. Organizations must also ensure workers continue to use good practices and receive additional security education as their roles change or become increasingly sensitive. With more than five million individuals working for state governments and 14 million working for local governments, the task of doing so is not trivial.

Comply with a plethora of mandates. Tax offices, health and human services agencies, police departments, payroll departments and other organizations that handle sensitive information are subject to a range of federal regulations, including the Payment Card Industry Data Security Standard (PCI-DSS) and the Health Insurance Portability and Accountability Act (HIPAA), as well as newer regulations such as IRS Publication 1075, Criminal Justice Information Security (CJIS) and the European Union's General Data Protection Regulation (GDPR). While many of these mandates require costly governance, protection mechanisms, and auditing and reporting capabilities, federal legislation does not usually include funding to cover the staffing or toolsets required. These unfunded mandates — along with a shortage of personnel skilled in deploying these controls — place an additional burden on IT departments.

Stretch budgets further. State and local governments are allocating more dollars to cybersecurity as threats and attacks increase in the public sector. In 2017, cybersecurity was expected to be the top area of increased funding in state and local government.[10] Even so, organizations are still under pressure to cut costs, and security budgets are a relatively small percentage of spending in government organizations.[11]

THE PROBLEM WITH "SECURITY AS USUAL"

Given these challenges and the current threat landscape, traditional security methods have become obsolete.

THE THREAT LANDSCAPE: DATA BREACHES AND RANSOMWARE TOP THE LIST

The threat landscape is constantly evolving and cyberattacks against government are becoming increasingly targeted and stealthy. Hackers now use social engineering and other tactics that prey on legitimate users to gain entrance into an organization's system. Once in, they may dwell there for months or even years. In a study by the Ponemon Institute, the average time to detect a data breach was 191 days, and the average time to contain a breach was 66 days.[14]

In the past year, data breaches and ransomware have become the most prevalent attacks on government organizations, with espionage being the top motive (64 percent) followed by financial gain (20 percent). Other motives included hacktivism and grudges.[15]

Espionage-related data breaches. Public sector organizations were the third-most targeted victim of data breaches in 2017, according to Verizon's annual data breach survey.[16] More than 21,000 incidents were reported among 92 public sector organizations surveyed, with 239 of those incidents resulting in a confirmed data breach. Forty-one percent of the data stolen was personal data, 41 percent was "trade" secrets, 14 percent was credentials and the remainder was medical. More than 90 percent of the actors were affiliated with foreign governments, and phishing was a favored tactic. Perhaps most concerning is that in almost 60 percent of cases, it took years for the breaches to be discovered.

Ransomware. In just three years, ransomware moved from the 22nd-most common type of malware across

RANSOMWARE REPERCUSSIONS

In late 2017, a ransomware attack on Mecklenberg County, N.C., online systems occurred after a phishing email was used to gain access to an employee's network login credentials. Knowing that it could restore its systems and applications by using backup files, the county refused to pay the ransom. The attack affected 200 systems and froze many online public services — including a jury management application, an employee payment platform and several programs at the Department of Social Services.[12] Three weeks after the attack, only 80 of the services had been restored, providing insight into the time, complexity and personnel costs involved in recovery operations of this magnitude.[13]

industries to the 5th-most common in 2017; in 2017, government organizations became the No. 1 target of ransomware attacks.[17]

While hospitals, schools, state legislatures, counties and cities have been targets, smaller U.S. police departments have been hit particularly hard — partly because many are still running outdated systems that are no longer included in vendors' security patch cycles. Those who have refused to pay a ransom have still paid a price. In one high-profile case, a police department in Texas lost eight years of digital evidence after refusing to pay.[18]

Hacktivism. State and local governments are increasingly the target of hackers motivated by ideology, politics or social issues. "It's hacking for a cause, and it's exploding," says Lohrmann.

Hacktivists have defaced websites, hacked into email and publicly disclosed it, crashed systems and more. Some industry experts fear hacktivists may find their way into critical infrastructure, disrupting utilities, emergency systems and other essential services.

OUTDATED TACTICS INCREASE VULNERABILITY AND UNDERMINE SECURITY

In spite of their determination to protect today's sprawling ecosystems, many IT leaders use tactics that undermine their goals — or fail to implement tactics that could significantly improve their security stance.

Overemphasis on prevention. Until recently, cybersecurity arsenals were heavy on firewalls, intrusion detection systems, proxies, email filtering, web filtering and other prevention tools, and security teams spent the majority of their time and resources keeping people out of the system. As the first line of defense, prevention is essential. In this new era of the extended enterprise and stealthy, protracted data breaches, however, an overemphasis on prevention is a misuse of resources. That's because these tools don't protect data once a hacker makes it into the system. Modern security requires a more balanced distribution of resources across prevention, diagnostics and monitoring, and response and mitigation. IT leaders are beginning to recognize this, as indicated by a recent SANS Institute survey, in which respondents planned to spend twice as much on detection and response as on protection and prevention.[19]

Reliance on one-time audits and annual risk management review. Today's threat environment is evolving too rapidly and criminals can move too quickly for organizations to go a year without assessing security controls and risk. Without continuous monitoring and analysis, hackers can get into the system, stay longer and do more damage.

Using compliance as a benchmark. While regulatory compliance is an important business requirement, many organizations make the mistake of using it as a benchmark for security rather than a starting point. According to the Capability Maturity Model Integration (CMMI)®, compliance with key mandates would be considered the lowest level of risk management and compliance maturity.[20] More mature security strategies incorporate defense-in-depth, risk-driven priorities and sustainable risk management. The most mature level is business-driven security, where business priorities drive security strategy.

Failure to use existing controls. Although most organizations have encryption mechanisms, they aren't always encrypting data at rest — even though doing so could prevent a system intrusion from becoming an actual data breach, where data can be "read."

Other missed opportunities for stronger security include the failure to:

- Use multi-factor authentication (MFA) to add another layer of security to user authentication by having the user supply something they have (e.g., a one-time password provided via text message or email) in addition to something they know (i.e., a user name and password).
- Routinely patch all systems, software and devices on an ongoing, systematic basis.
- Automate threat analysis from server to endpoints.
- Provide ongoing awareness of phishing attacks and other prevalent threats.

GOVERNMENTS ARE TRANSFORMING THEIR SECURITY PRACTICES

To modernize security and transform government, forward-thinking IT leaders are adopting a resilient, adaptable and unified approach that helps them gain

greater visibility; quickly identify and respond to risks; minimize exposure; and meet business needs for agility, efficiency and cost savings.

RESILIENCE FROM THE GROUND UP

Transformative security aims for simplicity and resilience by building security into the organization from the ground up. In doing so, it addresses key challenges of the extended IT ecosystem. It allows state and local agencies to support thousands of devices, processes and applications, as well as protect and manage data whether it is on premises, in the cloud, on a device or somewhere in between. Security is built into everything, including core servers and storage; laptops, desktops, mobile devices and other endpoints; and physical and virtual networks. User authentication, access control, encryption and other protections are provided to ensure only authorized users can access and manipulate data regardless of where it exists. Finally, mechanisms and processes exist to recover data in the event of a data breach or loss.

ADAPTABLE, ADVANCED SECURITY OPERATIONS

Transformative security is adaptable, alleviating the burdens of manual management and freeing cybersecurity staff to focus on what matters most. It allows security personnel to see across the ever-changing threat landscape, and then agilely evolve programs and controls as needed. It also allows organizations to more easily and securely build or optimize their own security operations center (SOC), consume SOC capabilities as a service or adopt a hybrid approach that allows both. Key components of adaptable, advanced security operations include:

- Converged visibility across devices, hybrid/cloud-based applications and virtual infrastructure
- Threat intelligence and advanced analytics to understand trends, actors, vulnerabilities and threats
- Rapid response and remediation to quickly detect threats and accelerate response via automation and advanced analytics

UNIFIED RISK MANAGEMENT

Transformative security helps state and local IT leaders see the "big picture" so they can better identify, contextualize and prioritize risk. It also helps organizations unify security practices. In doing so, organizations can accelerate and improve decision-making, better control overall business risk, and prepare for compliance with government and internal regulations.

BEST PRACTICES FOR SECURITY MODERNIZATION

The following best practices can help state and local government IT leaders modernize security and solve some of their most pressing IT challenges:

Go back to basics. Update policies, procedures and documentation to reflect the realities of protecting data in an extended ecosystem, and then use these policies as the foundation of your security program.

Start with a thorough risk assessment. Locate and identify the organization's most sensitive data and understand how it is protected. Compare existing mechanisms to industry best practices and your updated policies, and then build a plan to get to the new model. It's okay to use cyber insurance and regulatory compliance checklists to begin the conversation, but remember that compliance is the most basic stage of a mature security model.

Make continuous risk assessment a mindset. Implement continuous data monitoring and conduct a weekly risk management review that focuses on critical services. Use "tabletop" exercises and "what-if" scenarios to regularly test cybersecurity and incident response plans.

Centralize governance. As state, county and local IT systems adopt cross-jurisdictional systems, centralized cybersecurity governance will become increasingly important to get an accurate view of risk and ensure consistent application of security controls.

Build a culture of security awareness. Make sure all end users receive security awareness training, including executives and other senior-level staff. Help people understand their role in mitigating risk — whether they're interacting with people, processes or a specific device.

Establish metrics and scorecards. "Management needs to know where they're at and how they're doing," says Lohrmann. He recommends that organizations establish a baseline that documents how well the organization is currently doing security-wise; identify goals, metrics or leading indicators for measuring progress; perform penetration and other tests to verify controls are working as expected; and use a dashboard to keep track of progress over time.

Choose stable, experienced vendors. Consider the maturity of the vendor's business model and whether it has the stability to stay in business over many years. Does it have deep and broad expertise in cybersecurity? Does it have experience in the public sector? When you procure new services and technology, what protections are built into the offering and what pieces will need to be added?

IN SUMMARY: MODERNIZATION IS A TEAM SPORT

To better serve their constituents, attract and retain the workforce of tomorrow, meet regulatory requirements, control costs and address other challenges, government IT leaders need a modern cybersecurity approach that is resilient, adaptable and unified. This approach turns security into a key business enabler, allowing organizations to agilely, cost-effectively and securely fulfill their missions while meeting business goals. To that end, it's important to draw on business and security expertise when moving into the future.

"A lot of people are so focused on security that they underestimate the importance of relationships and working as a team. Or, they don't understand the business of government or what the business folks are thinking about," says Lohrmann. "On the other side, you may have people who have great relationship skills and understand how government works, but they don't understand the risks from a security perspective. You can fall off the horse from either side. Leaders need to understand these risks and address gaps as needed."

Besides building relationships across internal teams, Lohrmann advises forming partnerships with the private sector as well as other governments. "You have to have relationships," he says. "A CISO will fail on an island."

This piece was developed and written by the Center for Digital Government Content Studio, with information and input from Dell EMC and Intel.

ENDNOTES

1. www.nascio.org/Portals/0/Publications/Documents/2017/NASCIO-TopTen-2018.pdf
2. https://betanews.com/2017/04/27/us-government-data-breach/
3. Symantec. Internet Security Threat Report. April 2017.
4. Ponemon Institute. The Economic Risk of Confidential Data on Mobile Devices in the Workplace. February 2016
5. https://newsroom.accenture.com/news/accenture-survey-shows-us-citizens-want-more-digital-services-from-their-government.htm
6. www.herjavecgroup.com/wp-content/uploads/2017/06/HG-and-CV-The-Cybersecurity-Jobs-Report-2017.pdf
7. Center for Digital Government interview with Dan Lohrmann. January 2018.
8. http://statescoop.com/local-government-agencies-remain-concerned-about-lack-of-cyber-awareness
9. www.govtech.com/security/Can-Security-Awareness-Training-Change-Behavior-and-Reduce-Risk.html
10. www.govtech.com/budget-finance/IT-Spending-in-State-and-Local-IT-What-Does-2017-Hold.html
11. SANS. IT Security Spending Trends. February 2016.
12. www.charlotteobserver.com/news/politics-government/article189428824.html
13. www.mecknc.gov/news/Pages/Countywide-system-outage.aspx
14. The Ponemon Institute. 2017 Cost of Data Breach Study. June 2017.
15. Verizon. 2017 Data Breach Investigations Report. 10th Edition. April 2017.
16. Ibid.
17. Ibid.
18. https://nakedsecurity.sophos.com/2017/02/01/eight-years-worth-of-police-evidence-wiped-out-in-ransomware-attack/
19. SANS. IT Security Spending Trends. February 2016.
20. http://cmmiinstitute.com/capability-maturity-model-integration. Accessed January 2018.

PRODUCED BY:

CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. The Center conducts e.Republic's annual Digital Cities and Counties Surveys; the biennial Digital States Survey; and a wide range of custom research projects. **www.centerdigitalgov.com**

FOR:

DELL EMC

Dell EMC and Intel brings innovation to government organizations of all sizes so they and their citizens can transform and thrive in the digital economy. Becoming a digital organization means transforming operating models, people, and process as well as IT. Intel integrates security technology into their products and creates specific cybersecurity hardware and software under the Intel Security brand. Dell EMC uniquely powers this digital transformation by delivering best-in-class technology for applications, data, infrastructure and security – from the edge to the core to the cloud. Collectively under the banner of Dell Technologies, Dell, Dell EMC, Pivotal, RSA, SecureWorks, Virtustream, and VMware align to deliver a singular goal: helping governments transform the way they work, so they can transform the lives of the citizens they serve.

intel

Intel and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.