CDW·G PEOPLE WHO GET IT®

MANAGING CYBER RISKS IN A PUBLIC SECTOR ENVIRONMENT

As threats evolve and IT infrastructure changes, governments seek technology that can adapt to new challenges.

EXECUTIVE SUMMARY

In the wake of recent high-profile data breaches at the Office of Personnel Management, Indiana's Medicaid program and other government entities, cybersecurity has moved to the top of the priority list for federal, state and local government agencies. The sense of urgency is building as agencies seek to avoid becoming the next cybersecurity headline.

Government technology leaders know, however, that cybersecurity can quickly become an all-consuming effort that requires significant resources. The challenge is to develop and implement a cybersecurity strategy that protects the agency and its constituents from breaches, but does so within financial and logistical constraints. Governments need holistic, cost-effective IT solutions that adjust rapidly and repeatedly to a constantly changing threat environment. This approach builds a robust, defense-in-depth approach to security that remains resilient against future threats.

Agencies build cybersecurity programs to protect the confidentiality, integrity and availability of information. Increasingly, however, they are also faced with evolving regulatory frameworks guiding the selection, design and deployment of cybersecurity controls.

A Changing Threat Environment Requires Flexible Solutions

The changing threat environment is the main driver behind recent investments in cybersecurity by government agencies. Attackers are increasing their focus on government targets; technology environments are becoming more complex and prone to vulnerabilities; and attack tools are increasing in their sophistication and ability to avoid detection. Agencies manage most modern threats with a holistic, enterprise approach to cybersecurity, but legacy technology and slow adoption of modern IT solutions — some because of funding and acquisition considerations — complicate the effort to secure data and systems. Malware, advanced persistent threats, the Internet of Things, legacy technology and insider threats are just some of the dangers agencies must protect against.

Malware: Malicious software, or malware, is perhaps the oldest cybersecurity threat, with viruses and worms tracing their roots back to the 1980s. The authors of malware keep pace with improvements in security technologies, and in an ongoing cat-and-mouse game, go to great lengths to keep a foothold in upgraded operating systems and applications by developing stealthier and more effective malware.

Some malware authors focus on compromising numerous systems, regardless of their owner or purpose. For example, CoinMiner malware infects systems via malicious code embedded in online advertising and then uses the purloined computing capacity to mine bitcoin or other cryptocurrencies. Similarly, the Kovter Trojan infects systems via malicious email attachments and then generates advertising revenue via click fraud schemes. These unfocused malware attacks are a nuisance to agency IT staff who must rebuild infected systems.

Other malware, however, has more focused purposes and can be dangerous on government computer systems. NanoCore, for example, is a remote access Trojan that allows hackers to gain complete control of infected systems, where they can then either steal sensitive information or use the system as a jumping-off point for attacks on the rest of the network.

Ransomware is a specific type of malware that poses a significant threat. After ransomware infects a target system, it uses strong cryptography to encrypt the contents with a secret key. If the victim wishes to decrypt the information and regain access, he or she must pay a ransom to the attacker. Recent ransomware outbreaks, such as WannaCry and Petya, found victims at all levels of government, ranging from Britain's National Health Service to local law enforcement agencies across the United States.

Advanced persistent threats: Government agencies are often the targets of extremely talented attackers and well-funded attacks known as advanced persistent threats. These attackers, typically sponsored by nation-states, are quite patient and focus on very specific targets. Once they gain access, they operate with stealthy techniques, placing a high priority on avoiding detection. During the 2015 OPM breach, attackers believed to be associated with the Chinese government operated within the agency's network undetected for more than a year, stealing massive quantities of sensitive personnel information. In 2018, the U.S. government accused Iran's Mabna Institute of conducting a four-year-long attack in at least 20 countries against hundreds of universities and dozens of government agencies, including the U.S. Labor Department, the Federal Energy Regulatory Commission and the states of Hawaii and Indiana.

The intelligence community believes that during the 2016 U.S. election cycle, APT attackers associated with the Russian government gained access to computer servers belonging to the Democratic National Committee and used the information gained to discredit the Hillary Clinton presidential campaign. Researchers also believe that Russian operatives successfully targeted and scanned voting systems used by many states.

Internet of Things: State and local governments are embracing Internet of Things sensors and devices to enable smart city initiatives, improve their agencies' environmental efficiency and increase public safety. Similar initiatives in the federal government also promise to dramatically improve the quality of service provided to residents, but all these projects come fraught with new cybersecurity risks.

The Impact of Cybersecurity Breaches

Government agencies occupy a unique position of public trust. They collect, create and curate sensitive information ranging from the capabilities of military weapons systems to the financial information of individual taxpayers. When cybersecurity breaches undermine the security of that information, the resulting loss of trust may be substantial.

The Department of Veterans Affairs saw this in 2006, when the agency reported that a laptop containing the sensitive information of 26.5 million veterans had been stolen from an employee's apartment. The agency later agreed to settle a class-action lawsuit for $20 million.

In early 2018, state and local governments across the country reported data breaches both intentional and accidental. An email hack at the Idaho Transportation Department made public the Social Security numbers and credit card information of truckers who registered their rigs in the state. Davidson County, N.C. and the city of Atlanta were each targeted by ransomware that brought their computer networks to a halt.

In 2013, hackers linked to the Iranian government compromised command-and-control systems supporting a small dam in Rye, N.Y. They were unable to take physical control of the dam only because an important control cable had been disconnected for troubleshooting purposes. This attack, however, points out critical deficiencies in IoT security measures — including an increased reliance on cellular networks, which are more visible to would-be attackers and often less protected — and a focus on targeting IoT systems by state-sponsored attackers.

Legacy technology: One often-overlooked threat to cybersecurity comes in the form of legacy systems, which were designed to operate in a completely different threat and technical environment. Their lack of modern cybersecurity controls provides hackers with an easy path into government networks. Agency technology staff should search all systems for outdated hardware and software that may require upgrading or replacement.

As agencies seek to replace legacy technology, they also often undertake digital transformation initiatives that upgrade and enhance technologies. Recent examples of these initiatives include the Next Generation 911 and FirstNet programs, which are designed to enhance public safety communications efforts nationwide.

Insider threats: While cybersecurity teams often focus on the ominous threats posed by external and foreign attackers, risk often comes from within. Employees with legitimate access to agency systems may misuse that access for financial gain, to satisfy their own curiosity or to engage in industrial or foreign espionage.

In 2017, three employees from the inspector general's office at the Department of Homeland Security were accused of stealing an agency computer system containing personal information on more than 246,000 DHS employees. Their motivation was not identity theft; instead, they were searching for test data they could use to develop their own version of an agency case management system, which they could market to other government agencies.

Not all insider breaches are malicious, however. The state of Kansas revealed the last four digits of Social Security numbers for thousands of state employees and candidates for office on the secretary of state's website. It also gave Social Security numbers for about a thousand voters to the state of Florida as part of an effort to cut down on voter fraud; those numbers also became public.

The Journey Begins: Infrastructure That Adapts

IT modernization is the foundation upon which government security rests. The need for updated and properly integrated systems drives funding requests and agency spending. However, these initiatives may also introduce vulnerabilities by expanding network footprints and creating integration challenges among vendors and services. The advent of the Internet of Things, cloud storage and other external services result in an increasingly blurred network perimeter, making it difficult to apply traditional perimeter-based security controls.

As government agencies increase their digital transformation and modernization efforts, they must choose multilayered security solutions that not only provide an effective defense against modern threats but also keep an eye toward the future. Agencies adopting a defense-in-depth approach to cybersecurity will find themselves well-positioned to combat these future threats.

For example, an agency may wish to harden its endpoints against external intruders while making sure that routine patch management activities close security weaknesses within the network. At the same time, agency cybersecurity teams should monitor user behavior and other patterns of activity on the network, watching for anomalies and outliers that may indicate insider misuse or external attackers.

Malware protection: As many security threats arrive via malware vectors, agency cybersecurity teams should ensure that they are taking proactive, detective and reactive steps to protect systems against malware-borne threats. These controls should include deploying frequently updated anti-virus protection on servers, endpoints and network gateways. Agencies should also consider the use of advanced botnet and malware detection tools that incorporate threat intelligence information and provide a robust defense against evolving threats.

User training: Cybersecurity starts and finishes with the user. No matter how robust an agency's cybersecurity controls,

Staying Ahead of Cybersecurity Threats

The greatest challenge facing cybersecurity professionals is the constantly changing nature of the threat landscape. Designing security controls that focus exclusively on the threats that exist today leaves agencies vulnerable to the unknown threats that will arise tomorrow.

Many cybersecurity controls provide strong adaptable defenses against unknown threats. For example, application control technology that uses whitelisting to identify the types of software permitted to run on a system will likely be able to block any malicious application created down the road. Similarly, intrusion prevention systems that leverage user behavior monitoring have a strong chance of detecting any anomalous activity, even if it is a previously unknown method of attack.

Threat intelligence products fill in the final piece of the threat puzzle. These solutions offer cybersecurity analysts up-to-date information on new and emerging threats, helping them stay ahead of the adversary.

a single mistake by an end user can undermine those efforts, providing attackers with access to sensitive information or granting them a foothold on internal agency networks. Combating these efforts requires regular security awareness training that helps users understand the threats facing the agency and their individual role in protecting the confidentiality, integrity and availability of government information and systems. These efforts should include a particular focus on phishing and spoofing attacks.

Network monitoring: Network activity is one of the most important sources of information for cybersecurity teams seeking to maintain situational awareness and identify active threats. Network monitoring activities fit into two major categories: passive and active. Passive network monitoring simply captures network traffic as it travels from point to point and monitors it for unusual activity. Active network monitoring actually manipulates network traffic by injecting test activity onto the network and observing its performance. This also plays an important role in network troubleshooting and performance monitoring.

Network access control: In addition to regularly monitoring network activity, agencies should consider the implementation of network access control technology that regulates devices allowed to connect to the network. NAC technology permits agencies to require user and/or device authentication prior to granting access to wired and wireless networks as well as VPN connections. NAC solutions also provide posture-checking capability, which verifies that a device is configured in compliance with the agency's security policy before it is allowed on the network.

Endpoint protection: Once a device is permitted on the network, agency IT teams should ensure that it remains secure over time. Endpoint protection technologies extend beyond traditional anti-virus software to provide additional security tools, including automated patch management and application control. Patch management ensures that the operating systems and applications installed on devices receive current security patches; application control technology limits the software that may run on a device by either blocking prohibited software or only allowing preapproved software.

Next-generation firewalls: Agencies already use network firewalls to build perimeters between networks of differing security levels — in particular, separating an internal network from the public internet. Firewalls operate based on rules that allow administrators to define authorized traffic and block anything that doesn't match those rules.

Next-generation firewalls (NGFWs) enhance traditional firewall technology by providing administrators with additional flexibility. While traditional firewalls are limited to rules based on network characteristics, such as IP addresses and ports, NGFWs provide additional context, allowing administrators to create rules based upon the identity of the user, the nature of the application, the content of traffic and other characteristics.

Secure web gateways: Malicious websites are a significant source of security incidents. Users are tricked into visiting a malicious link and then either fall victim to password phishing attacks or have malware installed on their systems. Secure web gateways offer a solution to this problem by providing administrators with an opportunity to control the websites visited by network users. They act as a proxy, making requests to web servers on behalf of end users and perform filtering to remove malicious traffic and block access to known malicious sites, preventing users from accidentally harming agency security.

Data loss prevention: Agencies can restrict the flow of sensitive information outside of controlled environments through data loss prevention systems. These systems may reside as a hardware appliance that monitors network traffic, a software solution that resides on endpoints and monitors user activity or a cloud-based solution that filters email and web traffic. DLP technology identifies sensitive information using two primary techniques. The first, pattern recognition, understands the formatting of sensitive data elements such as Social Security or credit card numbers and watches for data matching those patterns. The second approach, watermarking, applies digital tags to sensitive files and then watches for those tags leaving the secure network in an unauthorized fashion.

Internet of Things security: Modern networks are becoming increasingly complex as agencies deploy Internet of Things solutions in support of smart office programs, smart city initiatives and public safety programs. These IoT solutions use a broad network of sensors that require the same monitoring and maintenance as any other networked device. They often contain embedded operating systems that require security patches; left unmaintained, these may serve as access points

Security Success in Missouri

Michael Roling, CISO of Missouri, has experienced tremendous success building a cybersecurity program in his state. Roling brought together security and technology leaders from across state agencies to create a set of shared strategic cybersecurity goals.

Missouri has led the way with cybersecurity awareness training, creating a comprehensive awareness training program that has already reached over 40,000 state employees. That's just one component of a strong state security infrastructure that includes advanced malware protection solutions, a statewide vulnerability management program and the management of security solutions from over 30 vendors.

for intruders. Before deploying any IoT solution, agencies should ensure that they have appropriate security controls in place to segment IoT from other networked devices, controlling access and maintaining a secure operating environment.

Security analytics: The security infrastructures deployed by government agencies generate massive amounts of information. From anti-virus alerts on endpoints to intrusion alerts on the network, cybersecurity analysts must handle a deluge of information. Security information and event management solutions help manage this problem by receiving and aggregating information from a wide variety of security tools. They also use artificial intelligence and machine learning algorithms to correlate information received from different tools, watching for signs of compromise that might otherwise go unnoticed.

Security assessments and penetration testing: Even the most well-designed security infrastructure experiences issues. From accidentally created firewall rules to undetected software vulnerabilities, unexpected events can create sudden and significant cybersecurity risks. Agency cybersecurity teams should complement existing security controls with a set of security assessment tools designed to continuously evaluate the security of their infrastructure. Vulnerability management systems scan networked devices, searching for signs of vulnerabilities and tracking remediation efforts. Software testing tools watch for critical flaws in production code.

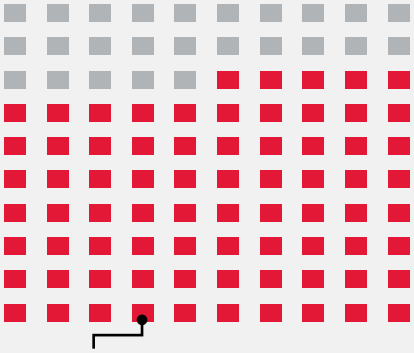
Penetration tests are the ultimate security assessment. During these tests, skilled cybersecurity professionals take on the role of an attacker and seek to break into a network using common hacking tools and techniques. If they gain access, they report back the vulnerabilities that they exploited, allowing agency cybersecurity teams to correct them and lower the risk of an actual attack.

The Journey Continues: Supporting Future Security

In addition to the changing threat landscape, federal, state and local government agencies must remain cognizant of existing and emerging compliance requirements that affect how they protect information and technology assets. Agency business and technology leaders must stay abreast of these requirements and ensure that they can operate in their own evolving technology environment in accordance with all relevant laws and regulations.

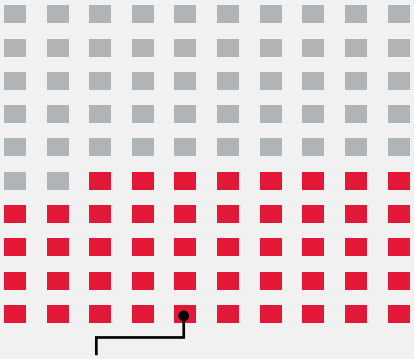
At the federal level, the president issued an executive order in May 2017 directing federal agencies to adopt a risk-based approach to cybersecurity and to immediately work to modernize cybersecurity controls. Federal agencies subject to this executive order should pay specific attention to the significant cybersecurity risks posed by systems with known vulnerabilities.

DHS' Trusted Internet Connections program seeks to provide a consistent level of security across agencies to ensure that all agencies have a secure, trusted path to the internet. The TIC initiative seeks to consolidate internet connections to a manageable number and then provide security services across those trusted connections. Recognizing the increasing shift toward cloud computing services, the federal government also now manages the Federal Risk and Authorization Management Program. FedRAMP provides a consistent process for the evaluation and approval of cloud computing vendors across federal agencies, relieving agencies of the burden of independently evaluating vendor security practices and providing a common level of vendor assurance across the federal government. And the Federal Information Technology Acquisition Reform Act (FITARA) of 2015 implements new requirements for the appointment of federal agency CIOs and the centralization of procurement practices.



75%

The percentage of government agencies without a separate cybersecurity function[1]



48%

The percentage of government employees who do not believe they're responsible for IT security[2]

While many of these regulations come from the federal government, state and local technology officials should also pay heed. Agencies interacting with the federal government must be able to integrate with these new, more secure systems. For example, the federal law enforcement community publishes the Criminal Justice Information Services (CJIS) Security Policy. This policy contains specific requirements for state and local law enforcement agencies seeking access to federal law enforcement systems.

State and local agencies may also look to the federal government for advice on security best practices. The National Institute of Standards and Technology publishes a Cybersecurity Framework (CSF) that provides comprehensive guidance on cybersecurity issues that can form the foundation of any cybersecurity program in the public or private sector. This framework classifies

Source: [1]Netwrix, "2017 IT Risks Report," August 2017; [2]Dtex Systems, "Uncovering the Gaps: Security Perceptions and Behaviors of Today's Government Employees," March 2018

cybersecurity activities into five major functions:

- Identify
- Protect
- Detect
- Respond
- Recover

The CSF then provides policies, standards and best practices for organizations to follow as they implement and manage each of those five cybersecurity functions.

Agencies that choose to adopt a well-defined framework such as CSF will increase their ability to future-proof their infrastructure against new and evolving cybersecurity requirements. By adopting a best-practices approach to cybersecurity, agencies will have a strong foundation in place when new requirements arise.

CDW·G: A Security Partner That Gets IT

More state, county and local agencies have hired CISOs, but they're still often short on resources needed to combat cyberattacks. In today's sophisticated threat environment, CDW's solution providers can serve as your organization's security partner. CDW·G takes a comprehensive approach to identifying and meeting the needs of every customer. Each engagement includes five phases designed to help you achieve your security objectives in an efficient, effective manner. These include:

- Initial discovery session
- Assessment review
- Detailed manufacturer evaluations
- Procurement, configuration and deployment
- 24/7 telephone support

CDW's experts conduct framework and compliance assessments that find areas for improvement and provide managed services in real time. Our other services include:

CDW Threat Check: This complimentary service, powered by state-of-the-art technology from CDW·G partners, can unmask undetected vulnerabilities on an agency network. Threat Check allows agencies to remediate deficiencies and return to their missions.

Comprehensive Security Assessment: This service examines every significant asset in an IT environment, including a password audit, penetration testing, website/application scanning, trust relationship analysis and wireless network assessments. The service includes a full analysis along with recommendations.

The CDW·G Approach

ASSESS

Evaluate business objectives, technology environments and processes; identify opportunities for performance improvements and cost savings.

DESIGN

Recommend relevant technologies and services, document technical architecture, deployment plans, "measures of success," budgets and timelines.

DEPLOY

Assist with product fulfillment, configuration, broad-scale implementation, integration and training.

MANAGE

Proactively monitor systems to ensure technology is running as intended and provide support when and how you need it.

Learn more about CDW·G's security solutions and services at CDWG.com/managerisk or call your CDW·G account manager at 800-808-4239.

Explore Our Featured Partners:

FORCEPOINT Platinum Partner | FORTINET | paloalto NETWORKS | Symantec

Learn more about the biggest threats facing organizations today and measures that can help protect your agency's data at CDWG.com/securityreport.

CDW·G PEOPLE WHO GET IT®