SECURING GOVERNMENT

LESSONS FROM THE CYBER FRONTLINES

CONTENTS

Executive Summary

Many **news outlets** declared 2014 to be "The Year of the Breach," especially for government. The title seems appropriate. Last year, the U.S. Postal Service (USPS), the Nuclear Regulatory Commission, the State Department, and even the White House fell victim to successful hacks that resulted in sensitive information being exposed to adversaries and the public.

And that's just the beginning. Nearly every state experienced a government network breach during 2014, while simultaneously managing disruptions in commerce caused by hacks of companies such as Home Depot, Staples, and Target. Even localities were not exempt — Rapid City, N.D., and Napa, Calif., are just two cities whose websites were hacked.

Nevertheless, maybe we should reconsider that title and be a little more optimistic. Instead of "Year of the Breach," can we consider 2014 to be the "Year of Lessons"? Maybe the "Year of Progress"?

While government-at-large certainly faced setbacks in the cyber world, many agencies also took great steps toward security. At the federal level, commitments were made and plans drawn to better equip smaller entities with the resources and strategies necessary to protect their networks. Locally, many organizations created new partnerships and streamlined their internal systems to achieve greater security at less cost.

This guide explores how local, state, and federal governments have learned from successful attacks of the past to bolster their cybersecurity today. In this guide, we:

- Describe the level and impact of advanced cyberattacks on government agencies.
- Discuss five cybersecurity tactics that the public sector has deployed to mitigate risk.
- Provide two case studies from government to illustrate each tactic in action.
- Detail lessons learned from these government tactics.

The numerous cyber incidents of last year prove there is still more government must do to secure our nation's networks. However, the case studies in this guide highlight that innovators in the public sector are already leading the way to enhanced cybersecurity.

THE CYBERSECURITY LANDSCAPE of government

the THREAT

46,160 CYBER INCIDENTS
reported by federal agencies to the U.S. Computer Emergency Readiness Team in 2013

782% INCREASE IN CYBER THREATS
to federal agencies between 2006 - 2012

61% OF EXPERTS
in technology and policy who predict a major cyberattack causing widespread harm will occur by 2025

the IMPACT

$194 AVG. COST
per lost or breached record for government agencies

$400+ BILLION ANNUAL COST
of cybercrime to the world economy (estimated)

182 THOUSAND
beneficiaries of Medicaid and the Children's Health Insurance Program who had their personal information stolen

25 THOUSAND
Social Security numbers compromised in a 2012 breach of the Utah Department of Health

50 MILLION
people in North America without power for as long as four days after an August 2003 cyberattack on the electrical grid

800 THOUSAND
employees who had their personal information exposed in a 2014 hack of the U.S. Postal Service system

6 MILLION
Social Security numbers exposed in a 2012 data breach of South Carolina's Department of Revenue

the RESPONSE

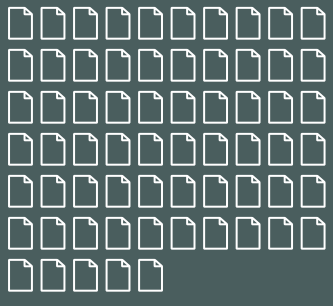
FOUR BILLS PASSED
related to cybersecurity, by the 113th Session of Congress (2014)

$65,000,000,000
Expected amount to be spent on U.S. cybersecurity contracts between 2015 and 2020, according to federal budget projections

$14,000,000,000
Amount requested in President Obama's fiscal 2016 budget for cybersecurity — a 10% increase from 2015

$35,000,000
Cost of the new Cyber Threat Intelligence Integration Center, which will be staffed by 50 employees

$2,000,000
Amount up for grabs in DARPA's Cyber Grand Challenge, which is designed to accelerate development of automated security systems



65 average number of pages in a federal agency's cybersecurity strategic plan

19 number of times "cyber" is mentioned in Obama's National Security Strategy released in February 2015, including in its own sub-section

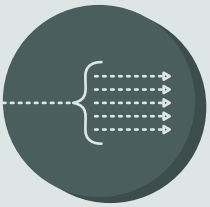
of federal agencies make no mention of cybersecurity in their Government Performance and Results Act strategic plans

of cyber intrusions go undetected by federal civilian agencies

6,000
number of people projected to work at the Defense Department's Cyber Command when it is fully staffed

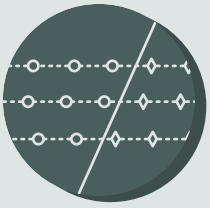
types of CYBERATTACKS

MALWARE
Malicious computer code used to corrupt, destroy, or steal digital information. Malware includes viruses and worms, in addition to spyware that monitors user activity and ransomware that holds data hostage



DISTRIBUTED DENIAL OF SERVICE
(DDoS) An interruption of network service, executed by sending such high volumes of traffic or data to a single network that it becomes overloaded and inoperable

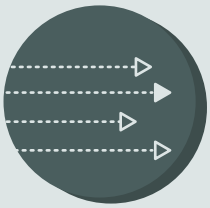
ADVANCED PERSISTENT THREAT
A continuous, sophisticated hacking process that allows an individual to enter and occupy a network for an extended amount of time in order to monitor or extract data from the target



STRUCTURED QUERY LANGUAGE INJECTION
An attack that alters a database search in a web-based application, allowing a hacker to obtain unauthorized access to sensitive information in a database

APPLICATION-LAYER ATTACK
An attack that causes fault in a server's operating system or applications, allowing an attack to bypass normal access controls to gain increased access to a system

INSIDER THREAT
Employee use of government personnel, facilities, information, equipment, networks or system to inflict harm on the United States. Insider threats can take many forms, from releasing confidential information to deploying advanced malware from within a network firewall



PHISHING
An attempt to extract sensitive information from an individual by masquerading as a trusted entity or person, usually via email or websites

SPAM
Messages sent or posted online that contain irrelevant, unsolicited, and often misleading information

types of HACKERS

CYBER CRIMINALS
Professional hackers who use malware, phishing, and other tactics for illegal monetary gain

INADVERTENT INSIDERS
Employees or contractors for an organization who compromise agency security through unintentional misuse of cyber systems

STATE OPERATIVES
Hackers employed by a nation-state to inflict military or financial harm on other nation-states via cyber networks

MALICIOUS INSIDERS
Employees or contractors of an organization who intentionally expose government information, systems, or personnel to external individuals

TROLLS
Individuals who target websites, social media accounts systems, or other online portals without damaging or exposing information for the sake of receiving recognition or expressing malice

HACKTIVISTS
Hackers motivated by political, religious, or personal beliefs to expose or deface cyber networks of perceived opponents

WHITE HAT HACKERS
Individuals who expose weaknesses in cyber systems for their private or public sector employers in order to remedy vulnerabilities before external hackers attack

SOURCES: GAO | Pew | Ponemon Institute | CSIS | Brookings | DoD | OMB | DARPA | FCW | Washington Post

We've Spent More Than 25 Years on the Front Lines.

Since day one, we've fought tirelessly to keep organizations and individuals from becoming targets of malware and cybercrime. Fast-forward 27 years, stealthy targeted attacks are on the rise, and our defense experience has paid off. McAfee® solutions—now part of Intel® Security—deliver exactly the kind of must-have technology high-assurance networks and organizations need to thwart today's targeted attacks. Learn more at intelsecurity.com.

intel Security

McAfee is now part of Intel Security.

Protecting Networks with Next Generation Firewalls

An interview with Ken Karsten, Vice President of Federal Sales at Intel Security

Because government serves citizens, agencies cannot achieve their missions without opening their secure networks to outside traffic. But this doesn't mean agencies must sacrifice security. It does mean, though, that organizations must have the policies and technologies in place to ensure this network traffic is diligently verified and monitored for appropriate use.

To understand how the public sector can achieve this network governance, we spoke with Ken Karsten of Intel Security, a security solutions provider. He explained how network administration is changing and why those changes require agencies to adopt next generation firewalls to ensure ongoing security.

CHANGES IN NETWORK ADMINISTRATION RISK SECURITY

First, Karsten explained that agencies are moving toward multi-disciplinary network management. "Decades ago, quality assurance was a different silo in a lot of manufacturing environments. But as quality went up, we started including that quality assurance in the regular manufacturing process. I think inevitably you're going to see the same with security. It's going to be a part of the intrinsic networking responsibility and IT environment," he said.

As a result, "Security people are going to require a better network understanding, and network people are going to require a better security understanding as [security solutions] are bolted in," Karsten added.

Second, Karsten said the transition of many agencies to cloud-based platforms will change the way networks are managed: "As you outsource to the cloud, many functions are being taken on by the cloud providers. Internally, administrators no longer need quite the breadth of technical capability to implement specific rule sets and policies of administration around these systems and capabilities."

"But what they will need is the ability to make decisions on what they want to allow or not allow, and how they want to leverage their technology and applications to drive their business objectives and their mission," said Karsten. As cloud providers perform many network tasks, traffic in and out of agency systems will naturally increase.

NEXT GENERATION FIREWALLS CONFRONT NEW CHALLENGES

According to Karsten, this increased traffic, coupled with the integration of security and network administration functions, requires agencies to adopt new firewalls.

"A traditional firewall basically allows traffic to go from inside to outside the network, and then from outside back into the network. And it does this based on a port and a protocol," he explained. "But what a traditional firewall really does is, based on a port, make an assumption of what that protocol is."

As the number of protocols exponentially multiply, it becomes easier for one protocol to trick the firewall into thinking it is a similar one by using the same port. Next generation firewalls mitigate this risk.

"When you bring next generation firewalls into play, you have the ability to do deep packet inspection. You know the protocol that the traffic is using, so you can ensure what it is, what application it's using, and which user is executing it," said Karsten. "It gives you a lot more granularity in policy, providing you a lot more visibility and security."

What's more, Karsten explained, "You can even go beyond that, to not only confirm that we're using a certain application, but also inspect it to see if there are any intrusions or misuse or even viruses in that application traffic."

This detailed visibility of network traffic also allows agencies to create more stringent policies regarding use and access. "The neat thing about a next generation firewall is not only does it have all these features and functions, but it also allows you to segment your network a little better. If you understand the internal environment — the applications that reside there and the users that are accessing those systems — you can create system-level access based on user," said Karsten.

"Then, if I see a person go through the firewall and see they're trying to access an application that they shouldn't not have access to, I can immediately know something is wrong and I can stop that traffic," he continued.

At the same time they segment their networks, agencies can also consolidate governance because the next generation firewall offers dual functionality. "It is both networking technology with security technology, housed in one form, factored both from a software perspective and a hardware perspective, even if it's virtual," said Karsten.

In summary, next generation firewalls meet both the operational and security challenges associated with the rise of network traffic. Karsten concluded, "Consolidating those features and functions lowers the total cost of an enterprise to implement a solution. It also raises the level of security by enabling additional security feature sets in real-time network traffic."

TACTIC #1:

Re-Secure the Sign-On Process

NIST AND DOD OFFER NEW WAYS FOR USERS TO ACCESS GOVERNMENT SERVICES

Verifying the identity of a user before they log in to a secure system is a necessary part of any cybersecurity strategy. However, when every agency or department requires a different set of credentials to verify individual user accounts, overarching security can actually decrease. Why?

Put yourself in the position of a citizen who routinely accesses multiple government services online. If you have to create unique passwords, security questions, and usernames for every interaction, you're going to find a way to ease your burden. You will probably create passwords that are similar or easily recallable. You'll also probably write them down to make sure you don't lose track of them. You might even create security questions that explicitly state your credentials, just to make it easier to get into the system and execute your tasks.

If login and credentialing procedures are cumbersome, users are more likely to create shortcuts to simplify the process. Unfortunately, those shortcuts compromise security by making it easier for hackers to obtain and leverage user identities. To help users and mitigate the risks of negligent accounts, government organizations are attempting to re-secure the sign-on process. Some are working to streamline the user experience, while others are doing away with passwords altogether. The two case studies in this section illustrate these tactics.

CASE STUDY #1: CONNECT.GOV

The National Strategy for Trusted Identities in Cyberspace (NSTIC) program office, part of the National Institute of Standards and Technology (NIST), is redesigning the way online government services are accessed. But rather than creating a single new tactic, NSTIC is acting as an idea hub by awarding grants for pilot projects that creatively authenticate digital identities.

One idea that's received significant support is **Connect.gov**, an initiative and portal focused on streamlining the access and credentialing process for citizens using government digital services. Rather than requiring unique passwords and biographic information, Connect.gov will pull credentials from a variety of existing online identification providers, including Google.

These credentials will be organized and managed by a USPS tool called the **Federal Cloud Credential Exchange** (FCCX). USPS describes FCCX as a "software middleman," because it will not use the credentials for USPS alone. Instead, other federal agencies can access and use those credentials to verify the identity of citizens accessing digital government services.

Currently, the pilot program is being tested at a small number of agencies, including the Departmetn of Veterans Affairs. However, the ultimate goal is to have the platform run on every secured government form and website. If that goal is achieved, citizens and agencies can expect immediate benefits.

Users will be able to access multiple agencies using a single set of credentials, which they can choose. This simplicity and choice offers an enhanced customer experience. It also makes it easy for users to securely maintain their online identity, because they have only one set of credentials to manage.

Participating agencies will be able to easily verify users' identity by checking robust credentials verified by third parties. They'll also be able to locally create a holistic identity management system because all of their user accounts will become standardized and centralized through Connect.gov. Finally, agencies can expect to spend less on endpoint security, because FCCX will bear the burden of maintaining credentials.

COGNITIVE FINGERPRINTS

CASE STUDY #2: DEPARTMENT OF DEFENSE COGNITIVE FINGERPRINTS

The Department of Defense (DoD) decided to take a different approach to securing login procedures for civilian and military personnel. During a department exercise, DoD's own cyber operatives — called "red teams" internally — were able to steal and use personnel's passwords to hack into defense networks with relative ease. This successful breach exposed a key vulnerability and emphasized the need to bolster the agency's credentialing protocols.

As former Defense Information Systems Agency (DISA) official **Michael Orndorff said**, "Running a system today that relies on passwords is as reckless as driving a car without brakes or headlights." Therefore, DoD has set a goal to eliminate password-based authentication protocols from its security procedures.

Initially, the agency worked to establish a public key infrastructure (PKI), which ties user identities to certain domains rather than to passwords alone. This is a good first step to security, but unfortunately it's not applicable to every technology system within the DoD wheelhouse. PKI also can't be used for interactions with private citizens untied to government domains. In those instances where PKI can't be leveraged, passwords still reigned supreme — until now.

Now DoD is exploring the use of behavioral profiling to verify user identities and fully replace passwords. Through a multimillion-dollar partnership with West Point, the department will discern how "cognitive fingerprints" can be established by analyzing the way users access information.

Habits such as typing speed, mouse cursor movements, and even typographical errors will be discerned and assigned to individual users. Once a behavioral profile is established, an automated system will be alerted when a person interacts with the system, either on a desktop or mobile device, in a different pattern.

Naturally, **some privacy concerns** are associated with the initiative because users won't be asked to create a cognitive fingerprint in the same way they would be asked to create a password. However, DoD hopes the benefits of this program — enhanced security, streamlined access, and easier transmission of encrypted information — will ultimately outweigh concerns.

BIG DATA ANALYTICS

CLOUD COMPUTING

CYBER SECURITY

DATA CENTER MODERNIZATION

MOBILITY & END USER COMPUTING

NETWORK MODERNIZATION

SECURE SOLUTIONS, SO AGENCIES CAN REST ASSURED

Government Acquisitions, Inc. (GAI) is a small business IT value-added reseller with 25+ years of experience. From fighting ATAs/APTs, to enhancing mobile security, to managing governance and risk – a mission mindset is in our DNA.

We work side-by-side with Federal IT teams and industry-leading OEM partners to modernize, optimize, and deliver unparalleled support.

Detect and Prevent. Enhance Security. Manage Risk.

Dedicated DNA. Mission Mindset.

Learn More About GAI's Cyber Solutions:
http://gov-acq.com/solutions-capabilities/cyber-security or call 513-721-8700.

Government Acquisitions

Featured Partner

Symantec

Crafting Holistic Insider Threat Protection

An interview with Prem Jadhwani, Chief Technology Officer of Government Acquisitions, Inc.

In addition to risking national security, insider threats are a serious vulnerability to intellectual property and classified information. No matter what the mission, every agency has high target assets that could be compromised. But how can an entire government network be secured against internal threats?

In a recent interview, Prem Jadhwani of Government Acquisitions, Inc. (GAI), a security solutions provider, asserted that agencies must first understand their current risk. Then, they should deploy a comprehensive, continuous monitoring program.

IDENTIFY INSIDER THREAT RISKS

Before tackling insider threats, Jadhwani said that agencies must first understand their critical assets, unique risk, and risk appetite. "Most of the time, people have the feeling the bad guys are going to come from outside, but they don't realize that there may be high-risk insiders who have certain behavioral patterns that are not being recognized," Jadhwani said.

Agencies must scrutinize the behaviors of insider threats, in order to develop a set of actionable indicators for cybersecurity teams. Jadhwani identified two patterns of potential indicators. The first are the virtual patterns that most companies already monitor to some extent. This includes digital log records that track employees' online activity.

"Are they going over to SharePoint sites loaded with classified data that they should not be touching? Do they have a need to know? And are they downloading or printing that data? Are they sending data to their personal emails? That's the digital trail, or virtual path, we look for," said Jadhwani.

The other side is non-virtual--what Jadhwani calls "people-centric"--that focuses on human behavior. Potential indicators of an insider threat include expressions of frustration or compulsive behavior, a tendency to work on-site or remotely at odd hours, signs of vulnerability such as drug abuse, and unexpected wealth acquisition or foreign travel.

Both virtual and non-virtual factors have to be monitored carefully over time, but this is no easy task. "You are collecting lots of structured and unstructured data and you need a way to be able to correlate that data over a long period of time and look at certain specific behaviors which will alert you automatically. Rather than just one specific behavior, you are better served to look for a pattern of behaviors that will help you identify a potential insider threat," said Jadhwani.

Once behavioral patterns are captured and analyzed, "normal behavior" baselines should be set. Then, deviations from that norm can alert your security team to potential threats in real-time using an integrated solution approach.

DEPLOY INTEGRATED SECURITY SYSTEMS

In order to establish this monitoring and alert system, Jadhwani said agencies will need more than just technology. "A lot of customers I speak to think that with think the technology is sufficient to protect against insider threats. However, I disagree with that," he said.

Instead, Jadhwani recommended taking a multi-faceted approach that he calls "PPTTC," for policies, procedures, technology, training, and continuous monitoring. The idea of this comprehensive approach is not just to detect threats within your agency, but to deter them.

"From Government Acquisition's perspective, we are a full set solution provider," said Jadhwani. "What that means is we start by gaining an understanding of a customer's environment, their tools, and their policies. And then we look at technology. But remember, none of the tools can do all the work alone. It's not about putting one tool here and one tool there. What you need to look for is a fully integrated and correlated solution architecture that spans multiple layers of security."

Training is another important component of this approach, Jadhwani said. Mandatory training modules that already take place in most agencies help build threat awareness into organizational culture. Product-specific training is also necessary so that tools, such as the monitoring dashboard described below, can be deployed effectively.

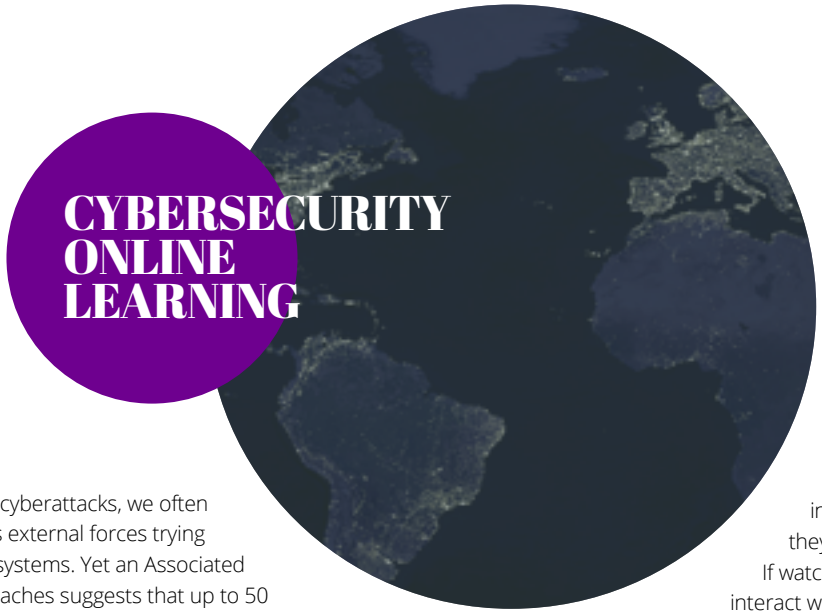
The final piece is constant surveillance of networks. "[Continuous monitoring software] collects, indexes, and visualizes the complete structured and unstructured data streams into one single pane which allows you to set your own rules and key performance indicators on a dashboard," Jadhwani explained. "It allows you to take real-time action before the damage is done." And a significant value-add of GAI as a solutions provider is that they can understand the infrastructure gaps, help provide valuable market research, and build a customized monitoring dashboard to fit an agency's specific needs.

Threats that have the potential to inflict significant damage require a security approach that is both meticulous and comprehensive. With the help of solutions providers such as Government Acquisitions, agencies can achieve this level of security and feel confident that their critical assets are protected.

TACTIC #2:

Empower End Users

STATE AND DOD TEACH THEIR EMPLOYEES TO TAKE SECURITY IN THEIR OWN HANDS



When we think of cyberattacks, we often imagine devious external forces trying to infiltrate government systems. Yet an Associated Press (AP) analysis of breaches suggests that up to 50 percent of federal cyber incidents are the result of misuse by employees or contractors who already have access to government systems. That means that agencies have a substantial opportunity to buffer cybersecurity simply by educating their employees to better handle sensitive information.

Empowering end users is a dual objective for government agencies. First and foremost, organizations must equip employees with personal best practices for safeguarding information. Additionally, user empowerment requires giving employees the knowledge and tools to prevent other users from endangering the organization's cybersecurity. The following case studies explain how two federal agencies have addressed these challenges by providing online training and tools to their employees.

CASE STUDY #1: STATE DEPARTMENT CYBERSECURITY ONLINE LEARNING

While all government employees are required to undergo basic security training, the constant evolution of cyberthreats means that education must continue beyond orientation. Consequently, the State Department produces an ongoing series of online workshops designed to supplement employees' FISMA-mandated security training.

Called **Cybersecurity Online Learning** (COL), the series provides detailed information to empower users — both at State and in other federal government settings — to protect their organizations. Because trainings take place in a virtual environment, they can be accessed from any location. If watched live, users can ask questions and interact with presenters during the demonstration. Programs are also offered on demand after the live session, to ensure maximum accessibility for government users.

The defining characteristic of the COL curriculum is its extensiveness. It covers a wide variety of cybersecurity topics, ranging from basic cyber diligence to mobile device security to phishing scheme identification.

And in addition to training on evergreen topics, the State Department also highlights context-specific concerns. For instance, last holiday season, the department launched **a special workshop** detailing how cyber criminals target gift givers with false gift card and charity scams in order to solicit bank account information. That sort of timely information ensures users are alert and able to recognize unique threats as they arise.

Moreover, COL varies its content to appeal to a wide audience, including employees working at any level of government and with any level of IT knowledge. For novice users, programs like "**International Advanced Persistent Threat**" increase awareness by providing an overview of basic cyber strategies. For more tech-savvy employees, workshops like "**Tracking Hackers**" discuss advanced tactics to thwart cyberattacks. Each course outlines the knowledge and skills required for participation so that potential users know which training is most appropriate for their level.

INSIDER THREAT TRAINING

Finally, trainings vary in format to complement user needs. Some presentations provide straightforward explanations of concepts, while roundtable discussions provide thought leadership and workshops provide hands-on tutorials. Therefore, users aren't relegated to one learning mode as they seek new information about cybersecurity.

CASE STUDY #2: DEPARTMENT OF DEFENSE INSIDER THREAT TRAINING

Of the cybersecurity breaches scrutinized in AP's 2013 analysis, 6 percent were attributed to employees or contractors who intentionally distributed government information to outsiders. These malicious insider threats are a unique challenge for agencies because both the warning signs and method of attack are different from the indicators most cybersecurity teams scrutinize.

To detect insider threats before they occur, it's necessary to recruit frontline staff in your efforts. On-the-ground personnel are best equipped to recognize and assess changes in behavior that may indicate an insider threat because they are aware of standard procedures associated with individuals and their roles. However, staff must know what to look for and how to respond when a threat is identified.

Recognizing this need for education, DoD's Center for Development of Security Excellence created a course for military and civilian personnel, contractors and volunteers regarding insider threats. "**Insider Threat Awareness**" takes an hour to complete and emphasizes the motto, "If you see something, say something."

The program begins by explaining the nature of insider threats — who commits them and for what possible reasons. It then showcases a series of real-world examples of internal breaches, highlighting the implementation of the attack, what led to its execution, and what outcomes the successful threat achieved. In addition to familiarizing personnel with the tactics of malicious insiders, these showcased incidents impress the importance of threat mitigation by detailing the consequences of insider threats.

After explaining insider threats, the course describes actions employees can take to proactively report and deter malicious insiders. Throughout the course, personnel are given scenario-based questions to test their retention of indicators and counter tactics. This training mechanism is crucial to ensuring that educated personnel are empowered to act once threats are identified.

Furthermore, to guarantee that employees are supported in their prevention efforts, the training is being integrated into a broader **DoD Insider Threat Program**, announced in September 2014. The new strategy is dedicated to synchronizing smaller programs across DoD's many departments in order to ensure threats can be identified and reported in a streamlined environment. It will certify that suspected threats are investigated by consistently monitoring and auditing source information for follow-up.

DoD is creating a holistic program to combat insider threats, because it recognizes that information technology and security staff alone cannot fight malicious insiders. Instead, the agency made it the job of every employee to be on alert for potential malicious insiders and then provided a framework in which employees can voice their concerns.

solarwinds DLT SOLUTIONS®

Mount A Better Defense For Insider & External Threats With SolarWinds® Cybersecurity & Continuous Monitoring Solutions

Cyber attacks continue to rise, and are a serious threat to our economy and national security. Agencies have an ongoing need to quickly defend against and respond to known **cybersecurity** threats, as well as recover from incidents, whether caused by careless or untrained insiders, malicious insiders, or malicious external threats.

Government IT professionals are responding to these growing cyber threats by deploying integrated security software, which also allows for continuous monitoring. Their IT operations, information assurance, and cybersecurity teams are well served with SolarWinds **IT management and monitoring software**, which can be used to proactively identify threats, take automated action to quarantine and mitigate damage, and analyze data to help prevent future attacks.

SolarWinds solutions use a unique "collect once, report many" strategy to address **continuous monitoring** across both IT Operations and Information Security domains in a single, cost-effective set of tools.

Join nearly every civilian agency, DoD branch, and intelligence agency in using SolarWinds to address IT management and monitoring challenges.

IT Management & Monitoring Solutions for Government

Go to
SOLARWINDS.COM/FEDERAL
to Download Fully-Functional FREE Trials

Network • Application & Server • Log & Security • Virtualization • Storage
Help Desk • File Transfer • Database Management

877.946.3751 • federalsales@solarwinds.com • solarwinds@dlt.com • LinkedIn

Supporting Insider Threat Identification with Continuous Monitoring

An interview with Chris LaPoint, Group Vice President of Product Management at SolarWinds

The risk of insider threats isn't anything new – recent breaches like WikiLeaks and Edward Snowden's exposé highlight the extreme risk of these types of security issues. However, Chris LaPoint of SolarWinds, an IT management and monitoring software provider, said that nevertheless, agencies are continuing to overlook insider threats when creating their cybersecurity strategy and technology architecture.

PRIORITIZE CYBERTHREATS

"If you look at where most agencies' budgets are aligned and where visibility is placed, the focus is really in response to high-profile, external attacks," said LaPoint. "One of the biggest risks is that there's so much focus around the external that people are forgetting about the internal. The conversation needs to consider all types of substantial threats and do so from both a tools and budget perspective."

According to a recent **survey** on cybersecurity threats by SolarWinds and research firm Market Connections, while agencies may not be focusing enough on the topic, cybersecurity personnel do recognize the risk of insider threats. Fifty three percent of federal IT professionals identified careless and untrained insiders as the greatest source of IT security threats at their agencies. More than half of respondents also said they believed the damage caused by malicious insider threats could be the same or greater than that caused by external threats.

Inadvertent insiders are also a significant risk. "Even if someone clicked on a link and inadvertently created an issue inside the network, that could lead to an inability to actually perform agency functions. That is a huge risk," said LaPoint.

"For external threats, you're obviously trying to keep the bad guys out of your networks, whereas internal threat prevention tactics tend to focus on training," he added. "But the common tactical thread for both is the ability to understand who, what, when, and where suspicious activity is taking place across the entire network."

DEPLOY INTEGRATED SECURITY SOFTWARE

Network monitoring is performed at many – if not all – agencies. However, LaPoint said that too often we only see compliance and security audits performed on a periodic basis – maybe twice a year – when monitoring should be continuous. "Agencies need to implement tools that allow for continuous monitoring so that those audits of access control and configuration are performed on an ongoing basis," he said.

SolarWinds' software provides the necessary tools to monitor and secure agency networks. These tools span three categories. First, "User and device tracking software offers the ability to understand where users are connecting to that network, where they've been, and what device they are using to connect, allowing for quick detection of any rouge devices that are connecting to the network," said LaPoint.

To consolidate this information, "Security information and event management software allows IT pros to collect data from all of the different systems, devices, and security appliances throughout a network," LaPoint explained. These capabilities alleviate the burden on agencies to independently capture and organize security data.

Then, "IP address management software helps IT understand where there are potential conflicts or issues on a network," said LaPoint. This functionality allows security staff to focus on high priority areas for remediation.

REAP ADDITIONAL BENEFITS

"Continuous monitoring software allows IT pros to take a more proactive and persistent approach in the same way that attackers are taking more advanced, persistent approaches to getting into the network," LaPoint said. Agencies can move beyond simply responding to threats by consistently monitoring behavior for indicators of future insider vulnerabilities.

LaPoint also explained how this last feature could aid non-security focused IT staff: "What an IT organization might be doing for continuous monitoring of security can actually complement what they're already doing on the operations side. The notion of being able to collect the data once and then use it for many different purposes is something we focus on." In other words, data collected with SolarWinds' software can be used to strengthen networks and operations at government organizations.

An integrated suite of monitoring solutions can help bridge the gap between IT and security personnel – a division which often hinders cyber strategies. "One of the things that we've really been trying to encourage IT professionals within government to understand is the need for IT operations and information security to work better together to reduce the number of tools and amount of data they're working with, while still understanding what's going on," said LaPoint.

The risk of insider threats has never been higher. For agencies to become truly secure, they will require integrated tools that not only protect the perimeter of the organization but continuously monitor internal cohorts and systems as well. Integrated software solutions are one way to consolidate security efforts, achieve continuous monitoring, and protect against insider threats.

PERSPECTIVE:

Cultivating a World-Class Cyber Workforce

AN INTERVIEW WITH LT. COL. VALERIE HENDERSON, SPOKESWOMAN FOR THE DEPARTMENT OF DEFENSE

Adapting and responding to the complexity of cybersecurity is a significant challenge for government agencies. However, cyber threats are not going to wait around for agencies to be ready, so it's crucial for government to get ahead of the curve. Focusing on process and technology can help improve cyber preparedness and response, but those don't mean much without people. Evolving threats call for a similarly evolving workforce. But what does this workforce look like? We spoke with Lt. Col. Valerie Henderson, spokeswoman for the Department of Defense (DoD), to get a better idea about how the department is addressing the critical issue of cybersecurity personnel.

"Effective cybersecurity requires various personnel with a wide range of knowledge, skill and abilities working in coordination with one another," said Henderson. "There is no such thing as a 'one-size-fits-all' cybersecurity professional."

Clearly, many skills are needed, but for strategic direction, Henderson explained that the DoD established the Cyberspace Workforce Strategy (DCWS) in December 2013. The DCWS is outlined through six focus areas:

1. **Establish** a cohesive set of DoD-wide cyberspace workforce management issuances.
2. **Employ** a multi-dimensional approach to recruiting.
3. **Institutionalize** continuous learning with greater focus on evaluating the maturity of skills.
4. **Retain** qualified personnel.
5. **Expand** threat knowledge.
6. **Understand** crisis and surge requirements and options.

Currently, the Department is in the process of implementing the DCWS beginning with Focus Area 1, said Henderson. The DoD will publish a cohesive policy for cyberspace workforce management, which scopes and defines the cyberspace workforce.

According to Henderson, the Department is also drafting a Cyberspace Workforce Framework (DCWF) – a lexicon of cyberspace roles – as another part of Focus Area 1. "The DCWF is the keystone to facilitate workforce transformation," she said.

To develop this framework, the DoD is leveraging the National Initiative for Cybersecurity Education (NICE) Workforce Framework. "The NICE Workforce Framework provides the structure and a significant amount of content to define these skill requirements," said Henderson.

The NICE Framework organizes cybersecurity into seven high-level "categories," with each one divided into several "specialty areas." Each specialty area identifies standard tasks and the abilities needed to successfully complete those tasks. For example, the category "analyze" contains the specialty areas of source intelligence, exploitation analysis, threat analysis, and targets. To break it down even further, the specialty area of exploitation analysis requires the task of, "Analyz[ing] collected information to identify vulnerabilities and potential for exploitation."

"The DCWF will establish an additional level of detail by identifying cyber work roles within each specialty area. This level of detail will enable DoD to establish workforce requirements, produce consistency and applicability of cyber skills and abilities, as well as promote a greater understanding of cybersecurity responsibilities as technology advances," Henderson said.

"The NICE Workforce Framework is currently limited to the cybersecurity workforce. DoD has established a set of definitions for the cyberspace workforce, which will be published in policy, DoD Directive 8140 – Cyber-

"Effective cybersecurity requires various personnel with a wide range of knowledge, skill, and abilities working in coordination with one another. There is no such thing as a 'one-size-fits-all' cybersecurity professional"

-Lt. Col. Valerie Henderson
Department of Defense

space Workforce Management," she said. "The definitions include an overarching definition for cyberspace workforce, and definitions for four skill-categories (cyberspace IT workforce, cybersecurity workforce, cyberspace effects workforce, and a sub-set of the intelligence workforce)."

By expanding the scope to address the entire DoD cyberspace workforce, the DCWF will facilitate:

- Career progression and assignment;
- Human capital planning; and
- Integration of cybersecurity responsibilities across the full-spectrum of the cyberspace workforce.

Furthermore, she added, "The DCWF and the processes it enables will allow the DoD to more effectively manage its workforce and thus mitigate personnel staffing issues." This is a very important task, as the DoD has noted "fierce competition" for the nation's limited pool of highly-skilled cyber professionals.

Finally, as stated in the DoD Workforce Cyber Strategy, Henderson emphasized that the department must seek to foster an environment where revolutionary innovation – enabled through cutting-edge technologies – produces a world-class workforce ready to meet any and all cyberspace challenges.

FireEye®
SECURITY REIMAGINED

ONE **UNIFIED** DEFENSE AGAINST CYBER ATTACKERS

Today's cyber attacks are targeted, sophisticated and focused on acquiring your most sensitive information. They also go undetected by traditional security technology. Government agencies and organizations need to reimagine security and adopt a Continuous Threat Protection model. This means having the ability to detect threats in real-time and reduce time to respond, thereby preventing or minimizing business impact. The FireEye Platform provides a multi-faceted approach to security – detect, prevent, analyze, respond.

DETECT

Signature-less and multi-flow virtual machine based approach that leverages superior threat intelligence

PREVENT

Multi-vector inline known and unknown threat prevention

ANALYZE

Containment, forensics investigation and kill chain reconstruction

RESPOND

Remediation support and threat intelligence to recover and improve risk posture

www.FireEye.com

Reprioritizing to Enhance Cyber Capabilities

An interview with Bob Lentz, Member of FireEye's Board of Directors, President of Cybersecurity Strategies, and former Deputy Assistant Secretary of Defense for Cyber, Information, and Identity Assurance

Though government spending on cybersecurity continues to increase, many agencies are having difficulty producing real return on their significant investments. Bob Lentz a member of the Board of Directors at FireEye, a security solutions provider, explained why allocation of security resources must change in the public sector. He also offered these three steps to enhance cybersecurity strategies.

UPGRADE YOUR TECHNOLOGY

"The first priority is that we need to move away from the legacy architectures and move to a much more advanced type of architecture to deal with the advanced cyber threats targeting agencies," said Lentz. "We can no longer invest in legacy instrumentation that is proven to be ineffective."

Simply put, legacy technology cannot meet the challenges of new menaces. "We are still focusing on what I would call ankle-biting attacks, and we're spending a disproportionate share of our resources on instrumentation to deal with these low level threats. But it's the more advanced attacks that are really having a significant impact on enterprises," said Lentz.

He explained that one reason many agencies continue to invest in ineffective systems is because they are too focused on regulatory compliance. "You might check a box that says you have to have identity management or access control. You check that box and you walk away saying, 'Well, I've met the spirit of the law.' In fact, it could be a very weak form of access control that does not adequately address an organization's threat environment. And unfortunately, this compliance mentality is creating a major gap where you're not really putting your best instrumentation and capabilities in place."

Instead of following regulations alone, agencies should invest in technologies that address their vulnerabilities. But before they do that, they have to assess their current state.

TACKLE YOUR VULNERABILITIES

"Priority number two is there needs to be very serious attention at the senior levels on regularly assessing your cyber readiness to deal with these attacks," said Lentz. "And that will result in having senior level oversight and, therefore, a corresponding increase in budget to be able to deal with those threats."

This oversight and budgeting should be dedicated to assessing current capabilities. "Agencies have to be much more rigorous in deploying red teams of their networks to assess their vulnerabilities," said Lentz. "If you constantly test yourself, you'll be able to know if you can contain these attacks and prevent them from getting to the crown jewels and causing significant damage."

At the same time, "You have to understand where your most important assets are," continued Lentz. "I think [agencies] will quickly come to the conclusion that even though they may be meeting these compliancy requirements, they're leaving themselves significantly open to attacks. So I think you really need to look deeper inside your network and shift your resources around."

STRENGTHEN YOUR SECURITY TEAMS

Finally, Lentz said that agencies must focus on filling the gap in cyber skills. He again related this need to inherited architecture problems. "What we have found is that we have a lot of these legacy capabilities that are pretty much taking over enterprises and, in fact, they're actually increasing the complexity of managing threats," he explained. "It's actually making the manpower and human resource problem much more weighty than it really needs to be."

Therefore, "The third priority is to focus on training the workforce and to leverage automated tools so that this workforce can focus on the increasing number of sophisticated, complex attacks," said Lentz.

As agencies transition technologies, they must also ensure they provide the necessary training to network administrators. "If you look at the breaches that are occurring, in some cases they'll have instrumentation that is pretty good, but they're just not using it right," said Lentz. Increased focus on personnel education can ensure technology investments aren't diminished by inappropriate use.

In addition to training for manual tasks, security should also be automated whenever possible. "Increased automation will allow you to make up for a lot of the talent gap," explained Lentz. "It will let you quickly sift through the noise, to look for those attacks that are going to be the most lethal. And then when there are attacks that are successful, you can more quickly stop them from having serious impact on your enterprise."

Lentz concluded, "You need to look deeply inside your network, re-architect your priorities, and invest in the right things. If you can do that, you'll implement the right techniques that will allow you to more effectively manage your enterprise and reduce the strain on human resources significantly."

TACTIC #3:

Partner with Others

DHS AND STATE GOVERNMENTS POOL KNOWLEDGE AND RESOURCES TO ENHANCE SECURITY

No matter how much technology, money, and staff you invest in cybersecurity, there will always be more that you can do to secure your organization. Simply put, the exponential growth in the number and complexity of cyberattacks means that there will always be a new threat requiring new counter tactics.

Unfortunately, agency budgets cannot ceaselessly expand as threats arise. This is especially true for state and local governments, whose smaller budgets and workforces are already strained to maintain a holistic security organization.

That being the case, agencies must shore up resources outside their four walls in order to constantly enhance their cyber toolset without dedicating more resources. By partnering with both public and private sector entities, government agencies can learn from others, share resources, and ultimately bolster their defenses. The two case studies in this section examine how government organizations on the state and national levels are using partnership models for security.

CASE STUDY #1: NATIONAL GUARD PARTNERSHIPS IN WASHINGTON AND MICHIGAN

Washington and Michigan are just two states that have endeavored in recent years to strengthen their network defenses with help from federal entities. But what sets these two states apart from their larger cohort is the means by which they coordinate with the higher level of government. Both states have partnered with their local National Guard.

In many ways, barriers to cybersecurity are different for state and federal governments. Funding and resources are the most obvious differentiators, with states maintaining smaller budgets and staff.

However, both levels of government face many similar challenges too. For instance, both a federal agency and a state's CIO office must coordinate across numerous departments to secure the entire organization. Both have to staff a robust cyber force with fewer resources than the private sector. Finally, both face cyberattacks that target secure networks with constantly evolving tactics.

Officials in states such as Washington and Michigan have recognized that these shared cybersecurity challenges outweigh governing differences and that, by partnering with federal agencies, they might learn common best practices while simultaneously supplementing their limited resources. So why not go directly to the federal government for support?

This is where the divide between state and federal becomes more evident. While the CIO reigns supreme at the state level of cybersecurity, there is no one-stop-shop for cyber on a federal level. The Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and many regulatory bodies have offered to share their best practices with non-federal organizations. But for a state office already burdened with financial and staff constraints, it can be challenging to access cohesive cyber resources from myriad intelligence, security, and defense agencies.

Enter the National Guard. The force's particular organizational structure and expertise in security make it an ideal partner for states hoping to reap greater resources from federal cybersecurity efforts.

The National Guard occupies a unique position in the hierarchical structure of government, because the federal and individual state governments dually employ the military force. As a result, the force already has the channels in place to coordinate with both government levels, making it the perfect body to liaise between the two. State offices can take advantage of these already established communication channels to better access federal information.

In addition to being the ideal link between state and federal government, the National Guard provides other benefits as a cybersecurity thought partner. Its expertise in disaster response, as well as its predefined coordination mechanisms with disaster response agencies at both levels of government, can buffer a state's incident response in the event of a

traumatic attack on a state's cyber system. Moreover, the National Guard maintains cybersecurity experts of its own who can offer their tested best practices, analyze states' cyber vulnerabilities, and even run cyber exercises for state systems.

The Washington National Guard provided the latter assistance for the first time in fall 2013, while Michigan's Guard partnership continues to focus on sharing resources and coordination efforts. On the whole, both partnerships have led to better-coordinated state cybersecurity efforts. What's more, the partnerships have encouraged other states — **most recently New Jersey and New York** — to consider how their National Guard can provide support for state cybersecurity.

CASE STUDY #2: DEPARTMENT OF HOMELAND SECURITY C³ VOLUNTARY PROGRAM

Even an agency as dynamic and robust as DHS can't secure every component of our nation's critical infrastructure from cyberattacks. In 2013, **Executive Order 13636** drew attention to this fact and also established expectations for how DHS could better ensure the ongoing protection of physical and virtual U.S. assets. The order stated, "We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."

DHS answered this mandate by creating the **Critical Infrastructure Cyber Community C³ Voluntary Program**. "C³" (pronounced C-cubed) is a nod to the three objectives of the program, **outlined by DHS**:

- **Converging** critical infrastructure community resources to support cybersecurity risk management and resilience through use of the [NIST Cybersecurity] Framework;
- **Connecting** critical infrastructure stakeholders to the national resilience effort through cybersecurity resilience advocacy, engagement and awareness; and
- **Coordinating** critical infrastructure cross sector efforts to maximize national cybersecurity resilience.

Put less alliteratively, the program is meant to merge local agencies and private organizations with federal DHS cybersecurity efforts. It will also provide a coordinating structure for that partnership.

As the name indicates, participation in C³ is voluntary. However, organizations have a lot to gain by using the program, since participation offers immediate access to multiple federal cyber resources and exposure to best practices from industry leaders and state and local governments.

The program focuses on three activities. First, it helps smaller agencies and large organizations implement the NIST framework by proactively providing risk-management guidance and sector-specific user support. Second, it creates a coordination point so that private organizations can find the cybersecurity information and guidelines they need without having to navigate multiple agencies. But in the true spirit of partnership, DHS also focuses on a third activity: using private-sector knowledge to buffer its own cyber defense mechanisms.

As stakeholders implement federal guidelines, DHS asks program volunteers to offer feedback about how their recommended cybersecurity tactics work in the real world, why they don't in some cases and, most importantly, what DHS can do to better safeguard the nation's cyber defenses. Ultimately, the partnership should buffer the ability of every participant — private sector organizations, state agencies, and DHS — to protect the nation's critical infrastructure from cyberattacks.

As DHS becomes more adept at coordinating among critical infrastructure stakeholders, it hopes to widen participation in the C³ Voluntary Program to include businesses of all sizes and any agencies involved in critical infrastructure cybersecurity.

PERSPECTIVE:

The Balancing Act of Performance & Security

AN INTERVIEW WITH DAVID L. STEVENS, CHIEF INFORMATION OFFICER OF MARICOPA COUNTY, ARIZ.

With limited funding and resources, how can local governments combat the wide array of sophisticated cyber threats? If major corporations and federal agencies are vulnerable, where does that leave a municipality?

We sat down with David L. Stevens, CIO of Maricopa County, Ariz., to gain insight into how his county and other localities can face this challenge and keep their networks secure. Key takeaways involved planning, automating, and measuring your cyber strategy while simultaneously ensuring it's not an impediment to public operations.

PLANNING AND AUTOMATION

No matter what level of government you secure, breaches will inevitably occur. Stevens understands this and, accordingly, has established a response plan to address them.

"For us, when laying the foundation for our cybersecurity strategy, a real priority was placed on our incident response plan," he said. "I believe it is a fundamental need that transcends the particular sector or business you operate in and government is no exception. Additionally, working with my Chief Information Security Officer (CISO), Michael Echols, and his team of professionals was essential for aligning services and risk and security management to our business."

A key component of cybersecurity operations is automation. Automation uses behavior-based analytics to automatically block certain attack types inline before they are able to circumvent network-based controls. Moreover, the correlation of events is necessary using Security Information and Event Management (SIEM) tools in an effort to demonstrate the scope of risk for systems that have been attacked and are known to be vulnerable to such attacks.

"These software packages are capable of automatically responding to potential threats as opposed to waiting for some sort of a manual intervention by a security analyst," Stevens explained. "This presents a significant value in terms of blocking threats as well as freeing up resources to spend more time, not reacting, but rather being proactive and in the hunt."

More specifically, Maricopa County leverages automated solutions to target and derail attacks before execution. "We have deployed Threat Emulation technology inline, so that it automatically stops malware from calling back to the Internet," said Stevens. "This is in opposition to what Target did, which is to detect the threat and then attempt to respond with a human being."

Threat Emulation technology identifies network threats and opens, or "emulates," them in secure, virtual "sandboxes." This inline deployment stops the malicious files and prevents them from escaping and breaching the network. Malicious file information is then shared so IT personnel can check the system for any other similar threats and avoid them in the future.

SECURING WITHOUT DISRUPTING

Keeping your network secure is obviously a key objective for a CIO, but security can't be so strict or complex that it creates a burdensome system for public employees.

"Deploying automated response technology was a risk decision given the impact that many intrusion prevention systems cause in environments, creating business issues, for example," Stevens said. "This may present a risk to users' ability to execute day-to-day work."

But Stevens has tried to find the right balance between security and ease of business. By frequently consulting with the CISO and referring to cybersecurity checklists from state and federal regulatory bodies, his office evaluates the amount of risk it's willing to take.

> ***"You need an honest assessment of your security operations, architecture, and governance up front."***
>
> -David L. Stevens
> *CIO, Maricopa, AZ*

"A 'hard stop' to any seemingly vulnerable operations is not a good solution," said Stevens. "Rather, you should define the risk and the potential liability so that you can make an educated decision."

Smart cyber strategy is also about developing clear expectations for employees, which helps reduce operational impediments. "The communication of the strategy to our employees and implementation of the technology has resulted in very few issues for users and the proactive mitigation of some potentially serious threats," Stevens said.

"We have also had great success in communicating to our users what the core threats are: malware, advanced persistent threats, and denial of service attacks," he continued. "We have gone to great lengths to get as many people as we can to understand those concepts, and it has resulted in them helping us identify threats where our controls may fail."

MEASURING EFFECTIVENESS

Communication, preparation, and automation are a few fundamental aspects of a cybersecurity strategy. But with scarce resources, how do you ensure that your strategy is working? What valuable metrics do your solutions demonstrate?

"You need an honest assessment of your security operations, architecture, and governance up front," said Stevens. You can evaluate your system using different diagrams or benchmarks, such as those from NIST. When you discover vulnerabilities, he suggested driving your investments and strategies toward improving those areas.

From a day-to-day operational perspective, Stevens utilizes dashboards the CISO prepared that help visualize and prioritize threats. He then looks at the most pressing, relevant threats and works with the security professionals to determine how many of those can be successfully dealt with by his security operation center or trusted business partners.

"We set key performance indicators for the security operation center and say, for example, out of 100 threats, you need to be able to respond to 95 of those within a determined period of time," he said.

By focusing on cyber preparedness and leveraging technological solutions that shore up personnel, Stevens highlighted how budget-constrained governments can make the most of their scarce resources. And by making network security a priority and an essential responsibility of everyone, along with planning and strong cyber professionals, government operations can continue to function without limiting business operations.

Better security for a better organization.

We help you provide the secure and compliant foundation to enable your agency to thrive.

Discover strong security that enables growth at Dell.com/security.

NSS Labs Next-Generation Firewall Product Analysis Report
Navigating the NIST Cybersecurity Framework
Cybersecurity Solutions for Government
Dell's NIST Cybersecurity Framework Self-Assessment Survey
How the Pentagon Can Tackle the Cyber Attribution Problem

DELL

Building Security into Agency Performance

An interview with Gene Stromecki, Federal Sales Specialist, and Dmitriy Ayrapetov, Project Manager at Dell SonicWALL

The IT landscape is more interconnected and complex than ever before. The increasing number of initiatives involving telework, bring-your-own-device (BYOD) and the Internet of Things (IoT) allow for greater employee flexibility, efficiency, and connectedness – but it also presents serious cybersecurity risks.

So how can agencies stay secure without hampering performance and service delivery? We spoke with Gene Stromecki and Dmitriy Ayrapetov, both from Dell SonicWALL, a network and security solutions provider, to learn more about the increasing complexity of federal IT. They also discussed why a holistic cyber approach is needed to stay secure and how solutions from Dell SonicWALL can help your agency meet the critical balance of performance and security.

PRIORITIZE CYBERSECURITY

An increasing complexity and the pervasive presence of threats require cybersecurity to be a primary consideration for agency leadership. "Security is no longer just an issue for the IT staff – it's now extending to the whole organization," said Stromecki. "The impact of [cyberthreats] can be substantial. In government, it affects reputation but also the ability of an agency to deliver on its mission of service to citizens." Illustrating this point, a McKinsey report found that cyberattacks could cost the world $3 trillion in lost productivity and growth by 2020.

Ayrapetov further emphasized the critical role of security in agency operations. "Security cannot be an afterthought; it has to be designed into all projects," he said. "With growing complexity, the risks become bigger and there are more entry points into the network. It takes just one slip-up in security to be compromised."

PROTECT THE ENTIRE DATA LIFECYCLE

To meet these difficult demands, agencies have to be persistent in their security efforts. They need to think about the entire lifecycle of their data and all of its potential end-points. "At the end of the day, security comes down to protecting the data," said Ayrapetov. "You need to start thinking about where the data lives: in servers, phones, computers, etc. When it lives in all those devices, how is it protected?"

For example, if a private contractor requests information, many questions need to be asked. What is being uploaded? Is the data going through an encrypted tunnel? Are credentials and access privileges being inspected? If credentials are stolen, is two-factor identification in place?

"Throughout the data lifecycle, we have to make sure that every step of the way is secure," said Ayrapetov. "If you are insecure by design, you will be breached."

VISUALIZE A HOLISTIC APPROACH

When there are so many moving parts and vulnerable access points, agencies need to look beyond individual network elements. With this in mind, government is adopting a holistic cyber approach.

"[The holistic approach] requires the need for sophisticated identity and access management tools, the ability to manage privileged passwords and privileged users, the need for technology such as encryption on the end-point, and of course the next generation firewall, where Dell is a leading provider," Stromecki said.

It is crucial for these tools to interoperate. "For example, an alert from a firewall allows you to disable a particular part of the network or particular endpoint devices in the case of an incident," he said.

Dell offers holistic protection by securing the network, user, data, and end-points. "Dell will monitor the network, help organizations create a plan and a security stance, analyze the security stance in an organization, and help respond to threats," said Ayrapetov.

Additionally, Ayrapetov noted that network monitoring can generate gigabytes of data per day, so Dell helps agencies pick out the signal from the noise in order to respond effectively to incidents.

ALIGN SECURITY STRATEGY TO ORGANIZATIONAL NEEDS

But while security is paramount, Stomecki and Ayrapetov both agreed that an agency that is completely locked down cannot function and carry out its mission.

"Dell's technologies have been optimized and engineered into systems to provide comprehensive and thorough components of security without substantially impacting network performance," said Stromecki. "Ultimately, networks are designed for their end users to be able to accomplish their tasks and the agency to fulfill its mission. Security – while essential – cannot bring the network to its knees."

Beyond simply deploying technology, government needs to weave these solutions into an overall environment of security, developing what Stromecki called a "security playbook." "[Agencies] need technologies that can detect compromises when they occur and understand the implications so that they can be contained," he explained. "Then, they need to move into a situation of detailed forensics that gets to the root cause of the event to understand it and prevent it from reoccurring. It's a continuous cycle."

By protecting networks and complying with security protocols without impeding agency performance, Dell facilitates an effective and holistic cybersecurity approach for government.

TACTIC #4:

Take an Enterprise Approach

NEVADA AND DHS INTEGRATE TECHNOLOGY AND STRATEGY TO ACHIEVE HOLISTIC CYBERSECURITY

Many large organizations face more than 1,000 cyberattacks per day that constantly evolve in response to the defensive systems they encounter. Agencies must move beyond traditional IT management, where threats are placed in silos based on particular types of attacks or targets.

A National Association of State Chief Information Officers (NASCIO) **report** explains how piecemeal approaches to cybersecurity are often unevenly applied, creating gaps in information and critical infrastructure security. Instead, a holistic view that offers economies of scale, eases administration, and improves responsiveness is necessary. This is the enterprise approach.

The most effective cyber **strategies** produce accurate assessments of the risks associated with each agency system and for the network as a whole. This enables greater visibility into your networks and better anticipation of and preparation for attacks. This transparency also facilitates greater resource allocation and prioritization.

Congress has emphasized the importance of this approach, setting aside **significant funding** for the Continuous Diagnostics and Mitigation (CDM) program — which we explore below. Our other case study examines the efficiencies the state of Nevada achieved via the enterprise approach.

CASE STUDY #1: NEVADA'S ENTERPRISE APPROACH

By 2012, Nevada had so many cyberthreats that it was hard for the state's IT department to keep up. Millions of daily attacks led to hundreds of security incidents while the state failed to uphold even standard security measures. Its cybersecurity strategy was in critical need of improvement.

Current Nevada CIO David Gustafson joined the state's **Enterprise IT Services** in 2009 and suggested utilizing an enterprise-level approach. Nevada Governor Brian Sandoval was onboard with this plan, and issued a directive calling for the state's cabinet to consolidate and integrate security under the office of Enterprise IT Services. This was a necessary but challenging mandate.

Prior to the governor's mandate endorsing an enterprise solution, agencies dealt with information security issues independently. To consolidate control with limited resources, Gustafson and his CISO Christopher Ipsen inspected the current IT infrastructure and prioritized their top four security concerns to address. These included application whitelisting to prevent unauthorized or harmful programs from running, patching applications, correcting system vulnerabilities, and restricting administrative privileges.

In addition to consolidating internal controls, Nevada officials deployed an enterprise approach for their user accounts. Previously, users accessed government information from disparate endpoints, with various credentials and login protocols. To provide greater perimeter security, Nevada applied a single solution that provided integrated security tools, automated access privilege workflows, consolidated reporting, and layered security across all endpoints.

This new enterprise approach can continuously monitor endpoint controls and attempted virus intrusions. With this information, state IT services can utilize event correlation, trending, and analysis to further understand and visualize state assets.

Today, more than half of Nevada's agencies are part of the centralized security system. The enterprise approach has led to cost savings, improved security, and increased business efficiencies. Over three years, Nevada paid **$1.1 million** to deploy security technology on 17,000 endpoints through an enterprise solution. The price would have been more than triple that (**$3.5 million**) if the state had purchased the solution for each agency separately — as was the standard procurement method. This ap-

CONTINUOUS DIAGNOSTIC & MITIGATION

proach not only saved money, but also has seen monthly security incidents decrease from 155 to 30 — an 80 percent reduction.

Piecemeal and decentralized cybersecurity approaches are costly and leave your network and your organization as a whole vulnerable, as Nevada's was only a few years ago. By recognizing the benefits of the enterprise approach, though, the state's information security is now much better. Educational institutions have also picked up on the trend. The University of Nevada at Reno has a newly established **Cyber Security Center** that largely focuses on a holistic approach to cybersecurity. Looking forward and knowing cyberthreats will only worsen, establishing comprehensive and dynamic enterprise strategies will help keep Nevada secure.

CASE STUDY #2: CONTINUOUS DIAGNOSTIC AND MITIGATION

CDM is a federal program that improves preparedness and reduces system vulnerabilities, so that that government can become more agile and efficient in combating cyberthreats. Similar to Nevada's approach, CDM provides a real-time, holistic view enterprise wide so agencies can understand the assets they have, the roles of those assets, and where risks are arising.

DHS established the CDM program, with guidance from the Office of Management and Budget (OMB) and NIST. For funding support, DHS' 2015 appropriations bill specifies that part of the **$140 billion** set aside for the Federal Network Security program should be used "to provide adequate, risk-based and cost-effective cybersecurity, including the acquisition and operation of a continuous monitoring and diagnostics program."

CDM helps federal agencies expand continuous diagnostic capabilities by increasing their network sensor capacity, automating sensor collections, and prioritizing risk alerts. To implement CDM, DHS first helps an agency set up the proper sensors to conduct an automated search for cyber flaws.

Once established, the data from these sensors feeds into a local dashboard and exports customized reports. The reports then alert network administrators to the most critical flaws and risks based on a weighted score, so they can appropriately allocate resources to mitigate flaws.

Finally, progress is tracked through dashboards and summary information can be shared among sister networks, and also fed into an enterprise-level dashboard. This process is repeated every 72 hours.

Full visibility into massive organizations in such a short time period can be very challenging. This is why prioritizing and leveraging technology is so important. According to **FCW**, there are three top priorities for CDM:

- **Automation** is the only practical way to assess all network assets every 72 hours. This would be virtually impossible for already resource-constrained agencies to do manually. Automation prioritizes events so only the worst require human attention, and also eliminates the threats that may require a response within milliseconds.
- **Continuous, real-time monitoring** prevents a threat that has entered a network from spreading and compromising dozens of machines. Continuous monitoring helps spot the breach quickly, so it can be contained and eradicated.
- **Big data analytics** draws insight from disparate data (mobile, sensors, e-mail, texts, images, phone logs, etc.), allowing staff to quickly connect the dots across different systems and applications in the IT infrastructure.

CDM is just getting started at many agencies, but those that have implemented the program have seen substantial benefits. For example, the State Department led the charge in 2008 with the first CDM-type program and has reported **reductions of up to 90 percent** in security risk. Furthermore, in a MeriTalk **study**, security managers praised CDM for its benefits, including less operational information security risk of IT systems (56 percent) and improved prioritization and risk management (55 percent).

To provide a consistent, government-wide set of CDM solutions and help other agencies achieve similar results, DHS and the General Services Administration (GSA) established an acquisition vehicle known as a blanket purchase agreement, or BPA, for continuous diagnostic capabilities. This way, all agencies can improve their cyber readiness and support adequate, risk-based, and cost-effective security solutions.

Assuming a Platform Approach to Cybersecurity

An interview with Pamela Warren, Director of Government and Industry Initiatives at Palo Alto Networks

Attackers use a multitude of tactics and applications to penetrate networks today – from sophisticated techniques to age-old cybercrime tactics such as drive-by downloads. In response, government agencies deploy a myriad of solutions, each serving a different security function. Yet even with these investments, organizations continue to experience breaches. Why?

To better understand the current cybersecurity landscape, we spoke with Pamela Warren of Palo Alto Networks, a provider of enterprise-level, next generation platforms. Warren explained that agencies often risk cybersecurity with piecemeal solutions for today's problems. She also described how a platform approach to security reduces risk, while adding value to an agency.

COMMON MISTAKES HINDER SECURITY

Warren explained that government organizations make four common mistakes when trying to secure their information systems. The most basic error, she said, is failing to have visibility to what is happening on your network: "What we're seeing is that many organizations are unaware of what applications they are even running on their network." This ends up being a major barrier to effective cybersecurity because it leaves unseen gaps in security for attackers to target.

But even for those applications that administrators do approve, Warren said they often don't contextualize their use. "Administrators aren't tying applications to users or user groups. They may whitelist certain applications to be used on their networks, but it's really the Wild West once the attacker is inside. So in the case of credential theft, if effective virtual segmentation by user or user group is not established, the attacker has unfettered access with that account."

Moreover, Warren explained, "Organizations believe that web and email are the only way attackers are getting in, and invest in security for just those vectors. But the next threat may use another application to get onto the network. One recent attack in critical infrastructure used an old token ring application within TCP/IP to launch the attack, for instance."

Agencies also often rely on disparate security solutions that don't work together to improve the overall security of the network. "[Agencies] apply a lot of security, but they're still coming up short," said Warren. "They acquire malware detection, firewalls, URL filtering, and advanced threat detection, but each one of those capabilities on their network is running almost virtually in standalone mode, even if they're using unified threat management."

Instead, security functions must be integrated and share insights in real time, to prevent zero-days and other attacks. "If one function is not informing the other, they're not necessarily any more secure," said Warren.

Similarly, intra-agency cohorts must work together. "We should be aggressive about security and feel like it's a responsibility we take seriously across the organization, regardless of whether it's the network team, the security team, the data center team, or the endpoint team," said Warren. But instead, "Groups are arguing over who has security, budget, and responsibility."

A PLATFORM APPROACH STREAMLINES SECURITY

In order to address these issues, Warren said organizations should assume a platform approach to security and employ a cohesive security strategy with distinct roles and responsibilities across all teams. This approach is in direct contrast to the disparate security products approach that some agencies take.

"[With a platform approach], you can simplify cross-departmental administration," said Warren. "You can centrally manage all security appliances and key security functions and unify your security policies, deploying your configurations and policies across all security functions. You can unify your enforcement capabilities across every aspect of your network and simplify the collection and analysis of logs from multiple locations. You can cover your internet edge, your data center, your mobile devices, and any other endpoints, regardless of how far-reaching your network is."

Furthermore, a platform approach to security simplifies network management and reduces product footprint. For example, one government customer had 80 different devices managing their network security. Palo Alto Networks was able to perform every function with just 8 platforms. In fact, Warren said the new devices actually stopped more threats than the systems they replaced.

A final benefit of the platform approach is its ability to break down barriers between security, network, and other IT teams. As security is coordinated and correlated across the network, Warren said departments can work more closely to ensure that the integration of security functions and visibility overcomes previous organizational siloes.

Ultimately, by organizing and monitoring an entire network through a platform approach, rather than a collection of individual security products, an agency can achieve more holistic and effective cybersecurity.

PERSPECTIVE:

Needed: Talent & Teamwork

AN INTERVIEW WITH MICHAEL COCKRILL, CHIEF INFORMATION OFFICER FOR THE STATE OF WASHINGTON

"The cyber threat is not just a bits and bytes threat, it's a threat to the continuity of commerce — of people being able to trade and do their jobs and deal with public safety issues."

- Michael Cockrill
CIO, Washington State

With conversations on cybersecurity often focused on the national level, you may expect significant differences between state and federal approaches to forming cyber strategies. However, Michael Cockrill, CIO of the state of Washington, said he faces many of the same problems as anyone else trying to defend an IT infrastructure. In discussing Washington's approach to cyber, Cockrill explained the basic strategies of the state as well as its role in protecting the "continuity of commerce" and developing a much-needed cyber workforce.

TOP-LEVEL OVERVIEW

Naturally, Cockrill's office focuses on three common cyber priorities: securing the state's cyber perimeter, making sure the state is aware when bad guys are actually in the system, and detecting and responding quickly to threats. These are the basic but essential steps in any cyber strategy. Cockrill also explained how CISO Agnes Kirk has been pivotal to the success of these objectives by focusing on the "fundamentals of network security as well as the evolving nuances" of cyber defense and understanding where the state's vulnerabilities are.

CONTINUITY OF COMMERCE

Another major focus of the Office of the CIO is what Cockrill refers to as the "continuity of commerce." This deals with the government's role related not only to the data that lives within the executive branch of government, but about the entire state and its critical infrastructure.

"It's the government's job to make sure that commerce can happen," said Cockrill. "The cyber threat is not just a bits and bytes threat, it's a threat to the continuity of commerce — of people being able to trade and do their jobs and deal with public safety issues."

Cockrill not only has to make sure agencies are securing their systems, but he must also set the appropriate policy framework to ensure other entities are taking other appropriate cybersecurity measures. The emphasis here is on securing critical infrastructure, especially monitoring and protecting the ports in Washington that are a giant choke point for commerce. Similarly, Cockrill explained the importance of having secure systems for dams so that "someone doesn't hack into them and open and close spillways."

The larger point is that in such an interconnected world where IT infrastructure underlies everything in the economy, there are significant vulnerabilities that must be addressed in a comprehensive, collective manner. The Office of the CIO has an important role to play in ensuring this is accomplished. "It's important for the government to secure vulnerabilities," said Cockrill. "But we also need to make sure that everybody else does their part to protect their zone of this interconnected economy."

CYBER WORKFORCE RECRUITMENT

To meet this collective effort, having an effective cyber workforce is crucial — but recruitment is not easy, to say the least. "The single hardest thing to find if you are a company of almost any kind today is an experienced CISO," Cockrill said.

With a dearth of cyber professionals in the United States and major Fortune 500 companies offering salaries in the high six digits, it is difficult for

government and smaller businesses to enlist experienced cyber professionals. "There are companies in our state that are going to Eastern Europe to hire their security people because we're just not creating enough of them out of our colleges," he said.

What's more, it doesn't help that cyber theft is a huge and growing business. "The black hats are multiplying rapidly but the white hats are tough to come by," said Cockrill.

But Cockrill is looking to tip the scales in the state's favor. The state of Washington is advancing the Public Regional Information Security Event Management (PRISEM) System: a shared regional cybersecurity monitoring system that aggregates and processes cyber event data, provides threat conditions, and extends situational awareness for public-sector organizations across the Puget Sound area.

The system is now being aligned with cybersecurity education in the state, providing students with access to real-time event data in an operational setting. Such exposure has helped contribute to esteemed cybersecurity programs in the state, such as the Center for Information Assurance and Cybersecurity (CIAC). "Every company needs some number of analysts who can just look at threat information and respond to it," said Cockrill. "So, we're taking a kind of 'grow your own' approach."

The state has also focused recruiting efforts at veterans. "Not everybody in the military gets trained in cybersecurity, but everybody that's coming out of the military has some level of training in security," said Cockrill. "That ingrained perspective of constantly doing threat assessment and constantly looking at adversaries outside your perimeter — that's the mindset an analyst or a defender needs."

With several major bases, the state has created a range of different programs to train veterans in cybersecurity. "We can build up that workforce to feed Washington businesses, so they're not having to go to Eastern Europe to find their security analysts," Cockrill joked.

He also noted the importance of cyber apprenticeships for the valuable experiences they provide and because they also trigger funding support from the G.I. Bill. "There's no certification or schooling that can compare with a couple weeks or months of actual live-fire data," Cockrill said.

When it comes to cybersecurity, everybody has a role to play. With a holistic view — focusing on the Pacific Northwest region all the way down to the latest information security graduate — Cockrill is helping establish a sustainable and secure future for the state of Washington.

TACTIC #5:

Prepare for Disruption

STATE AND LOCAL GOVERNMENTS PLAN FOR THE WORST TO MINIMIZE THE IMPACT OF ATTACKS

Ask any government cybersecurity professional what they would do if their agency experienced a breach, and without hesitation, they will respond, "It's not if, but when." The reality is that, despite our best efforts to deter or prevent attacks, the exponential growth in both the sophistication and number of cyberthreats will prevent agencies from ever being truly secure.

That doesn't mean government agencies should stop investing in cyber defenses. The tactics already discussed in this guide can, and do, safeguard against the majority of dangerous cyberattacks. Nevertheless, agencies must have a backup plan in place to minimize the disruption and fallout from those few successful hacks.

The case studies in this section examine how two public sector organizations have planned for the worst so they're ready to quickly counter the rare cyberattack that breaks through their defenses.

CASE STUDY #1: HOUSTON'S REGIONAL CYBER DISRUPTION PLANNING PROJECT

The Houston-Galveston Area Council is taking a multidisciplinary approach to cyber strategy through its regional **Cyber Disruption Planning (CDP) project**. The project is funded through the DHS Regional Catastrophic Preparedness Grant Program (RCPGP), though the Houston Office of Public Safety and Homeland Security directs operations.

The CDP project is focused on better integrating IT and emergency management teams in the Houston area. A **previous report** from DHS highlighted that IT departments could improve disruption responses by incorporating emergency management staff into their actions. Additionally, it states that many emergency management enterprises, "are not fully aware of their heavy reliance on the Cyber Infrastructure, nor have they studied the risk profile of critical cyber assets that support their operations."

To ensure that Houston can deploy a holistic counterattack in the event of a breach, CDP seeks to address this disconnection between emergency management and IT disaster personnel. The execution of cyber exercises and workshops with local and regional organizations is one way the CDP team hopes to connect services.

For instance, in November 2014, Harris County's Department of Education **held a planning exercise** to determine how it could best coordinate among participating jurisdictions in the event of a data center's operations being halted. Following the exercise, officials created a detailed report to emphasize major strengths, primary areas of improvement, and additional recommendations for the county to enhance its disruption plan. The report highlighted how cross-discipline training and an enhanced mutual understanding of emergency management and IT field practices could improve disruption response.

In addition to these exercises, CDP has **called for the creation** of Cyber Disruption Teams (CDTs) at all critical government agencies. These teams will comprise both IT and emergency management professionals and will serve a dual purpose. First, they will ensure that both skillsets are dedicated to cyber disaster planning. Secondly, they will increase awareness of the interconnectedness of IT and emergency management through iterative interaction between the two departments' staffs.

Finally, the CDP project team ensures that any lessons learned in government are accessible to private sector organizations in order to holistically prepare the region for attack. Through an online cyber disruption readiness assessment tool, Houston-area organizations can determine their preparation and response capabilities in the event of a significant cyber disruption. For those organizations that don't have a plan, the tool offers disruption templates to use for development.

Although the scope of Houston's CDP may be reduced to the urban area due to a decrease in funding for RCPGP, this tool can ensure that the region-at-large continues to improve its preparedness for cyber disruption.

CATASTROPHIC PREPAREDNESS INITIATIVE

CASE STUDY #2: NEW ENGLAND REGIONAL CATASTROPHIC PREPAREDNESS INITIATIVE

While Houston is focusing on its own locality, the Boston urban area decided to take a different approach to cyber disruption management after RCPGP awarded it nearly $1 million in 2010. It partnered with the city of Providence, the Commonwealth of Massachusetts, and the states of New Hampshire and Rhode Island to create a greater New England Regional Catastrophic Preparedness Initiative (NERCPI).

NERCPI seeks to coordinate a regional response plan for any kind of man-made or natural disaster and, for each scenario, it considers how cyber systems may be affected. These correlations were studied in the Cyber Disruption Response Project and resulted in a regional Resiliency Plan in 2012. This plan is being used by official participants of NERCPI, and was also distributed to many urban areas, states, and regional bodies.

Like Houston's approach, NERCPI's resiliency plan calls for the establishment of CDTs, and the integration of cyber and emergency management strategies. However, the regional CDTs are more dynamic to deal with a greater breadth of regional issues.

In addition to IT and emergency management personnel, each team incorporates public safety and service providers. Furthermore, teams are engineered to be scalable to the level of disruption. During catastrophic events, they can coordinate resources and information on a regional level. However, for minor local events, a designated team can deploy fewer resources with more targeted tactics.

The Resiliency Plan also required participants to collaboratively identify critical cyber assets and assess current cyber risks and capabilities. The results of these analyses were synthesized in a Regional Cyber Disruption Response Annex (CDRA). CDRA outlines the relationship between the entities and the support that each provides. It also provides a structured framework to coordinate cyber strategies across the region, in the event of a successful attack.

CDRA's tactics are bolstered by a series of "table-top exercises," similar to those in Houston. However, these take place on a larger scale. For instance, NERCPI once hosted a three-state regional exercise that tested responses of local and collective efforts to get computer systems back online after solar flares disabled them.

Leveraging a shared pool of IT, public safety, and emergency management staff is just one example of how a regional approach to disruption planning can enhance the resources available to each participant. Additionally, states and localities can share lessons learned from their unique experiences, creating a knowledge pool that is far richer than one entity alone could have achieved.

Finally, taking a regional approach to disruption planning allows individual entities to borrow resources from other less affected partners in times of emergency. For instance, following the Boston Marathon bombings, the city of Boston **received multiple offers** of assistance from other RCPGP-funded cities. Although this instance focused primarily on emergency management services, NERCPI anticipates that similar resource sharing would occur in the event of a cyber disruption.

Preparing Your Agency for Evolving Threats

An interview with Sean Applegate, Director of Technology Strategy & Advanced Solutions at Riverbed Federal

Cyberthreats are not static – they constantly evolve to target different vulnerabilities in new ways. Therefore, cybersecurity tools and strategies cannot remain static either. Yet many agencies struggle to match their cyber defense to the speed of their attackers.

To understand how agencies can integrate adaptive capabilities into their cybersecurity strategies, we spoke with Sean Applegate of Riverbed, a planning, configuration, and continuous monitoring solutions provider for large enterprises. He explained that an integrated suite of technologies will streamline threat analysis and prepare organizations for future attacks.

ACHIEVE FULL NETWORK VISIBILITY

Applegate outlined the steps to identifying, combating, and ultimately deterring cyberattacks. "It starts with understanding where you're at today and making sure that view of your infrastructure is maintained in real time. The easiest investments you can make early on are looking at ways to map your network and infrastructure, so you actually know what it looks like and how it is configured," he said.

Applegate added that one of the biggest barriers to effective security is having a top-down monitoring strategy that doesn't enable collaboration across organizational silos. When an agency is organized by department or technology stacks, working across teams often reduces time to detection and resolution.

"The goal of IT is to facilitate the agency mission," said Applegate. "And to do that, we must know what our infrastructure looks like, what normal business traffic and transactions look like, and then be able to work together when unusual events occur."

Riverbed's SteelCentral solutions can help achieve this goal. "Our tools can actually map and monitor every part of your infrastructure to let you understand exactly what the network and applications looks like, then allow you to manage change, track compliance, analyze real-time traffic and then conduct predictive analysis against that environment," explained Applegate.

As an added benefit, infrastructure threat and survivability modeling enables an agency to improve response plans by identifying key infrastructure weak points. "In a lot a cases, the same tools we use for network security monitoring are used for performance monitoring functionality as well. This enables agencies to extract more value from their investments," said Applegate.

CREATE A DETECTION AND MITIGATION PLAN

Once you've achieved full visibility of your network, "The next step is to understand what's actually transpiring from your clients to your applications or servers, or the Internet," Applegate continued. "Learning what's normal, how your applications communicate, how users access those, and their dependencies is critical for identifying unusual activities such as an advanced persistent threat (APT) or insider threat. Riverbed's SteelCentral solutions help identify when unusual activity is present."

Tightly integrated solutions and processes save time, a critical factor when combating an attack. "Riverbed's SteelCentral monitoring portfolio includes industry-leading flow, packet capture and application transaction analysis solutions," said Applegate. "Riverbed provides high level dashboards to use across the enterprise gain insight into both performance and security events, with the benefit of fast right-click drill-down to forensic details such as the packets or application transactions."

Identifying what's normal allows agencies to detect anomalies that indicate threats or intrusions. This detection should be followed by action. "The next step, in many cases, is getting to root cause analysis and containment," said Applegate. "Knowing there's an event is one thing, but quickly digging into the forensic details, determining scope and containment are key. Again, the right-click ability in our solutions makes it easy to analyze packets or application transactions in seconds, and if a zero-day event is present right-click to contain it by disabling the switch port it is connect to. For organizations comfortable with software-defined responses this step can even be automated for faster containment."

PROACTIVELY ANALYZE WEAKNESSES

A continuous monitoring platform, like that offered by Riverbed, provides agencies the capability to quickly react to threats. At the same time, an integrated suite of network mapping and monitoring tools allows government to proactively enhance security – as well as network operations. Providing a nice return on investment.

"If an organization wants to mature their practices, they can use the network planning and modeling functionality from Riverbed to conduct threat analysis modeling," said Applegate. "For example, you can use SteelCentral modeling solutions to execute threat modeling for common DDOS or amplification attacks, then analyze penetration depth, survivability based on response decisions or mission-impact on critical application performance. This enables leadership to contemplate, 'If we are being attacked in a specific manner, what's the specific impact on my mission and my operational capabilities?'"

By using an integrated set of visibility solutions, agencies can do more than just monitor and counter cyberattacks; they can also strengthen their defenses against future possible incidents.

CONCLUSION

The Way Forward

In this guide, we highlighted 10 case studies of government organizations that deployed dynamic tactics to enhance their cybersecurity. These initiatives ranged from simple and low-cost to complex and resource-intensive. But no matter the current state of cyber strategy or the extent of your resources and budget, there are key lessons that can be learned from these case studies and applied at your agency.

LESSON #1: YOU CAN'T DO IT ALONE.

The constantly evolving nature of cyber-threats means that agencies can't rely on their own efforts to keep up with security requirements. Instead, agencies must lean on one another, their employees, and industry to maximize cybersecurity capabilities.

Private-public partnerships can pool industry knowledge and supplement hard to come by resources, such as cyber personnel. Other agencies and levels of government can share best practices, act as a safety net in times of disruption, and provide templates for quick improvements to your network security. Even your own employees can provide an extra layer of defense when they're equipped with the skills to secure information and identify potential insider threats.

LESSON #2: CYBERSECURITY IS EVERYONE'S JOB.

These partnerships also highlight the expanding scope of the cybersecurity field. Today, cybersecurity is everyone's job.

Government cannot relegate cybersecurity to its IT personnel. Instead, every military and civilian employees must be educated to protect their organization from hackers and insider threats.

Similarly, private industry and local agencies must be equipped with the resources to protect themselves and our nation's infrastructure. As New England states and the Houston urban area recognized in their disruption planning, a successful cyberattack could not only affect IT, but also every other part of government operations. Therefore, emergency responders and public safety staff must also be ready to manage a cyber incident.

LESSON #3: COLLABORATION IS THE ONLY WAY FORWARD.

Although there are myriad technologies and strategies available to assist government's cybersecurity measures, there is only one way forward. That way is collaboration.

As hackers of all kinds attack every point of our nation's networks on a daily basis, it is imperative that government redefine the parameters of cybersecurity. To avoid another "Year of the Breach," every level and function of government must collaborate in order to pool resources and, most importantly, learn from one another.

LESSON #4: SAY GOODBYE TO SILOS.

Finally, to make the most of this multidimensional workforce, government must reorganize itself and its operations to coordinate efforts among disparate groups and levels of government. Silos must become a thing of the past.

Concerning operations, organizations must adopt an enterprise approach to security that allows them to view the entirety of their networks in order to immediately identify threats when they enter their system. Additionally, logins must be streamlined and integrated to better monitor access points and ensure users are safely accessing government services.

From an organizational perspective, agencies need new mechanisms and protocols that allow them to effectively work with other agencies and levels of government to counter cross-border threats and deal with disruptions. Internally, users must be empowered to work across departments to share information about systems and potential threats.

Acknowledgments

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 150,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to **info@govloop.com**.

GovLoop
1101 15th St NW, Suite 900
Washington, DC 20005
Phone: (202) 407-7421
Fax: (202) 407-7501
www.govloop.com
@GovLoop

ACKNOWLEDGMENTS

Thank you to Dell, Government Acquisitions Inc, Intel Security, FireEye, Palo Alto Networks, Riverbed Federal, and Solarwinds w/DLT Solutions for their support of this valuable resource for public-sector professionals.

AUTHORS:

Hannah Moss, Research Analyst
Matthew Garlipp, Research Fellow

DESIGNERS:

Jeff Ribeira, Creative Manager
Tommy Bowen, Graphic Designer
Kaitlyn Baker, Design Fellow

EDITOR:

Catherine Andrews, Director of Content

PHOTO CREDIT:

Alex
Andrew E. Larsen
Bert Kaufmann
Carla Vidal
DoD
Evonne
Kris Krug
Paul VanDerWerf
USDA
Washington National Guard

Notes

1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
@GovLoop