THE FUTURE OF CYBERSECURITY

Fifteen Trends Safeguarding Government

EXECUTIVE SUMMARY

Public servants have always been on the frontline of American defense, whether serving in combat positions or conducting analyses at a desk. They have long protected our infrastructure, economy, freedoms, and national interests. In the current age of cyber insecurity, those duties have never been more important.

Every employee at every level of government is charged with protecting our information from foreign and domestic hackers, who might use that information to harm or demoralize American systems. Furthermore, this protection only becomes more important each day as more people, places, and things are connected to the Internet.

As American government becomes increasingly connected, a question looms: How will our interests and information be safeguarded as cyberthreats mount and evolve?

Unfortunately, there is no silver bullet to cybersecurity. Instead, government will have to adopt multiple tactics that work in concert and evolve with new threat environments. In this guide, we explore the tools and strategies that public servants are using to safeguard our information systems.

To help you better understand the current cybersecurity landscape in government, we:

- Describe 15 trends shaping government cybersecurity in 2015.
- Hear insights from state, federal, and defense personnel on the current state of cyber initiatives.
- Predict how cybersecurity tools and tactics will change in the coming years.

Although cybersecurity will always be a moving target, government is taking action now to better protect our interests at home, abroad, and online. We explore the who, what, and why of that action.

CONTENTS

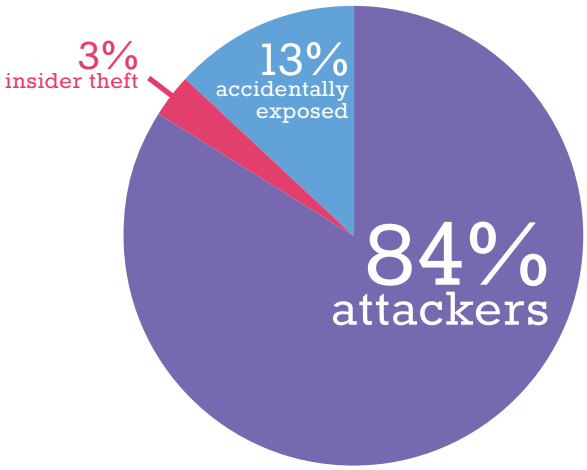
THE MOUNTING THREAT

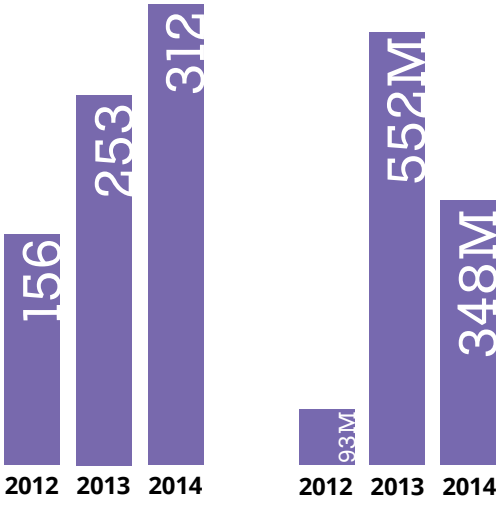
You already know cybersecurity is a big deal. It's in the news every day and your agency probably stresses its importance, too.

But do you know exactly how large the threat is to public sector organizations? Do you know how often hacks occur and what happens when they infiltrate a government network?

Before we dive into the trends shaping government cybersecurity, it's important to understand why cybersecurity is so critical and what's at stake when we fail. This section highlights some of the biggest growth areas and breaches in government cybersecurity.

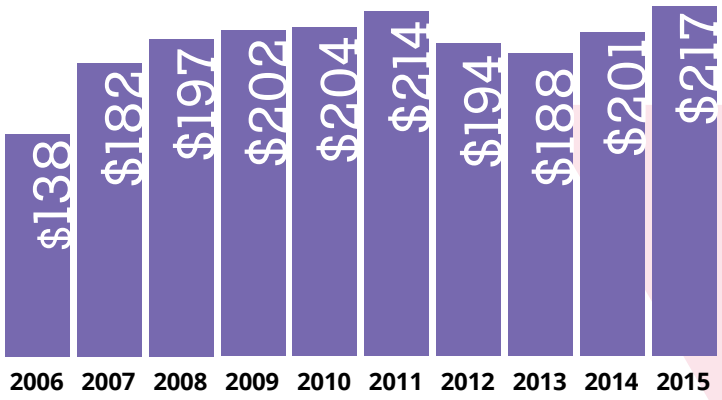
TOP CAUSES OF GOVERNMENT DATA BREACHES





TOTAL BREACHES

TOTAL IDENTITIES EXPOSED



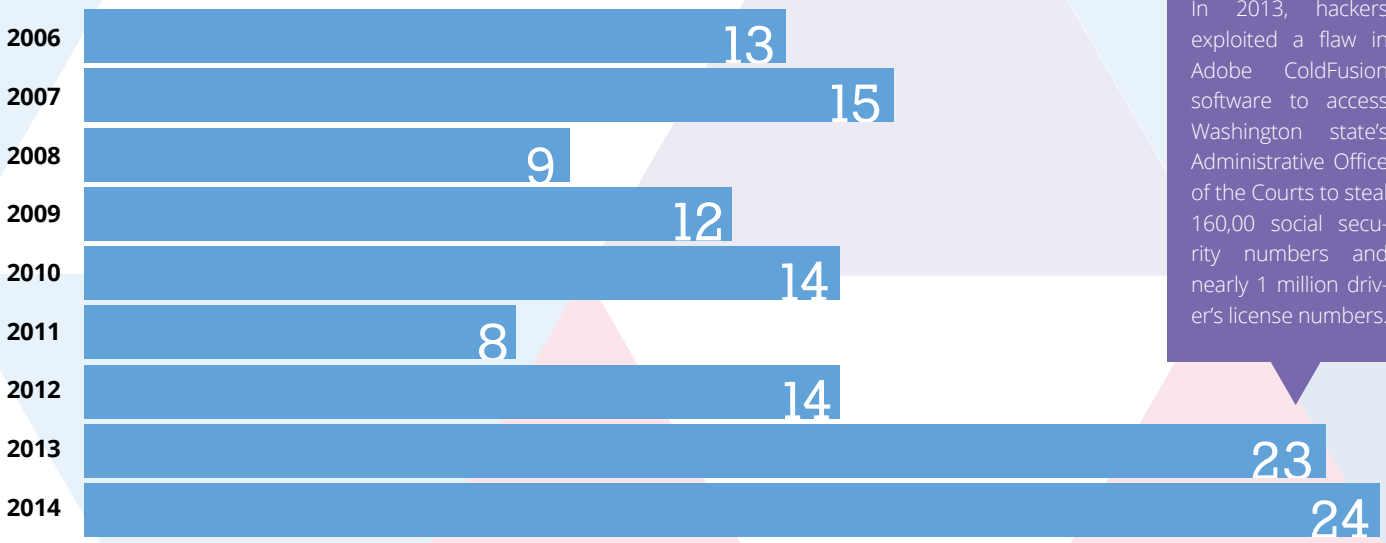
AVERAGE COST PER CAPITA

SPEAR-PHISHING EMAIL CAMPAIGNS, 2012-2014

	2014	Change	2013	Change	2012
Campaigns	841	+8%	779	+91%	408
Recipients per Campaign	18	-22%	23	-80%	111
Average Number of Email Attacks per Campaign	25	-14%	29	-76%	122
Average Duration of a Campaign	9 Days	+13%	8 Days	+32%	3 Days

In 2012 and 2013, a Nigerian man used phising emails to direct EPA and Census Bureau staff to mimicked agency websites, where they entered their login information. He used that stolen information to order agency office supplies that he then sold on the black market, costing both the government and agency vendors more than $1 million.

ZERO-DAY VULNERABILITIES



In 2013, hackers exploited a flaw in Adobe ColdFusion software to access Washington state's Administrative Office of the Courts to steal 160,00 social security numbers and nearly 1 million driver's license numbers.

Hackers linked to China breached OPM'S computer system using a zero-day vulnerability in December 2014. The breach exposed anywhere between 4 and 18 million individuals' information.

EMAIL MALWARE RATE

In August 2014, HHS announced that hackers installed malware onto the test code for HealthCare.gov. Investigators don't believe the hack specifically targeted the website, but the intruder nevertheless attempted to launch a denial-of-service from the host server.

RANSOMWARE TOTAL

In July 2014, the first file-encrypting ransomware for Android released an English version that used an FBI social engineering theme to demand payment from users. It also hijacked the device's camera to take a picture of the victim and assign that photo to the ransom note.

SOURCES

- Symantec Internet Security Threat Report 2015, Volume 20
- Ponemon Institute 2015 Cost of Data Breach Study: United States

solarwinds

MOUNT A BETTER DEFENSE

With SolarWinds Cybersecurity & Continuous Monitoring Solutions

Agencies have an ongoing need to quickly defend against, and respond to, known **cybersecurity** threats, as well as recover from incidents.

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 powerful, affordable, and easy-to-use solutions to make everything in government IT more secure:


SIEM: Log & Event Manager


Patch Manager


Network Configuration Manager


User Device Tracker


User Device Tracker


User Device Tracker

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 • LinkedIn

SAFEGUARDING AGAINST SHADOW IT

An Interview with Joel Dolisy, Chief Technology Officer and Chief Information Officer at SolarWinds

Increasingly, consumers want to bring their own technology solutions and devices into the workplace. However, "shadow IT" – unauthorized devices used within the workplace without the knowledge of the IT team – creates challenges for organizational cybersecurity efforts, especially in the public sector. In a recent interview, Joel Dolisy of SolarWinds, explained why we are seeing a rise in shadow IT and offered suggestions to address such cybersecurity challenges.

THE PROBLEM

Why exactly are new trends like shadow IT and mobile technology challenging cybersecurity efforts? The answers lie in the growing commercialization of IT itself.

"Everyone is using mobile devices nowadays," Dolisy said. "It's so pervasive that everybody believes they need to be able to use those devices at the office. Therein lies the problem. Because of the popularity of mobile technology and devices, you're going to try to use more IT capabilities that may not be secure."

Even public sector employees seem determined to use their mobile technologies in the workplace. But many don't realize the cyber risks they pose to their organizations, especially when IT departments are kept in the dark about the use of such technologies at work. This leads to loss of control of the cyber environment.

BETTER UNDERSTANDING OF THE END USER

Federal IT professionals need to identify triggers that cause users to implement their own unsecure mobile devices. Why do users seem willing to compromise their own security for their own tools?

Dolisy attributes this to the need to feel technology-forward. "They've all become IT managers in their own home, so they believe they know everything," he said. Users always want to feel like they have access to the latest gadgets. Sometimes, a user's need to feel technology-forward leads to the sentiment that they know better than their IT counterparts.

Dolisy also attributes the increase in shadow IT to convenience. "Security always takes a backseat to convenience," he said. "People like the convenience of being able to use their own devices and don't necessarily think about the consequences. They don't think about how someone can easily gain access to their devices from outside the organization."

Identifying triggers to unsecure mobile device use can help federal IT professionals better develop safe practices while ensuring their employees' technological needs are being met.

ACTIVE MANAGEMENT AS A SOLUTION

To better secure federal IT environments while accommodating people's need to use their own devices, Dolisy suggested focusing on the active management of endpoint security.

"You definitely don't want to micromanage everybody. But at the same time, you don't want to put your head in the sand and hope for the best," Dolisy said. "What you need to do is actively manage endpoint security by tracking new devices and networks. Your IT team needs to understand what devices are connected to your network, to whom they belong, and what they are accessing." Proactive monitoring from federal IT departments can enable employees to explore newer mobile technologies while maintaining information security for their organizations.

COMBATING COMPROMISING PRACTICES

In addition to proactive monitoring, Dolisy suggested two additional approaches to combat compromising behavior: awareness and network management. Awareness campaigns are excellent tools to educate employees about their mobile technologies and potential threats to cybersecurity. Network management ensures protocols are up to date.

"You need to make sure that there's an awareness campaign in place and that, in managing configurations, necessary devices are regularly patched, protocols being used are the latest versions, and ensure systems don't contain any vulnerabilities," Dolisy said.

He emphasized the importance of having strong policies in place for controlling access to your organization's networks. Such policies help IT professionals track who uses the network, how they access the network, and what devices they use.

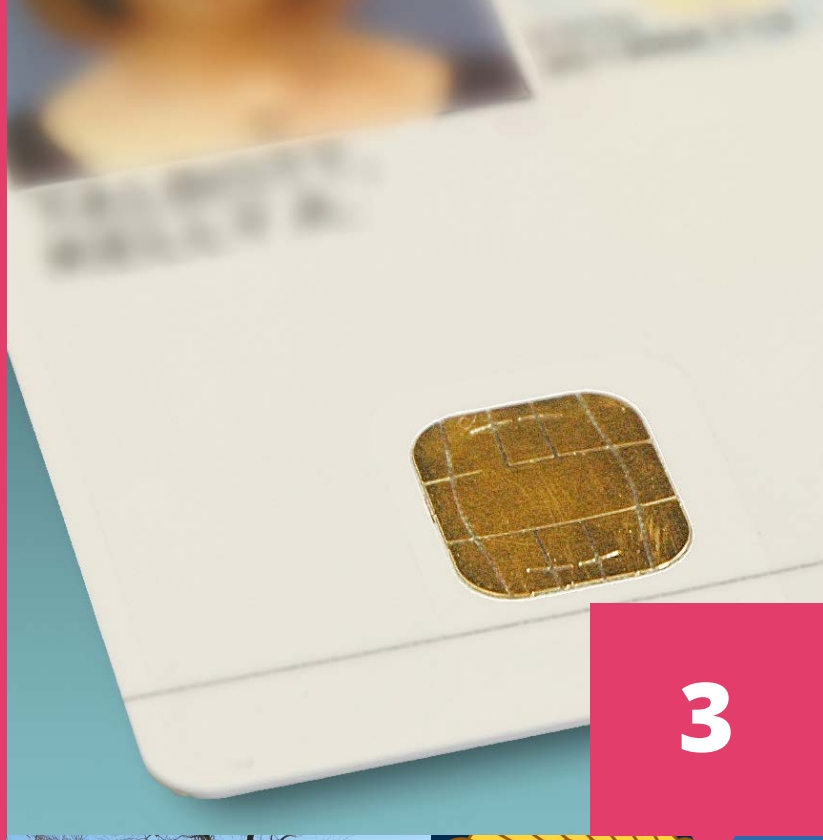
Finally, Dolisy recommended keeping tabs on public and private sector business cycles in order to identify strong partners for better problem solving. Organizations can keep up to date on cyber risks and mobile technology by learning best practices from third party organizations and identifying common vulnerabilities.

Dolisy concluded, "The whole concept of shadow IT is that you want it to be hidden. The best thing is to shed light on those behaviors and practices. If you're actively managing and monitoring, then you can move towards partial access of newer mobile technology and devices, which, in the end, will make your user happy."

A BETTER LOGIN

Security experts have long warned that passwords are among the weakest links in an organization's IT security structure. To combat that vulnerability, government often asks employees to create long, complex passwords containing a mixture of capital letters, numbers, and special characters.

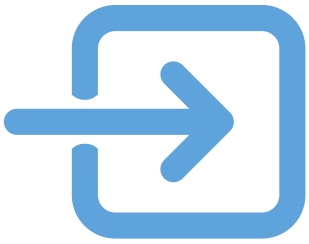
Still, as the 2014 "Year of the Breach" proved, these efforts are not enough to prevent cyberattacks. If anything, they increase insecurity because people are more likely to create easily recallable or duplicative passwords. As we continue into 2015, complex passwords are phasing out, ushering in a new era of innovative loginsf.



3

2

1



Trend #1:

FEDERATED IDENTITY SYSTEMS

Creating an identity management system that enables workers to use a single digital identity to access multiple resources across all organizations to which they're entitled

WHY IS IT IMPORTANT?

Federated identity systems (FIS) take identity management to the next level by negating the need for multiple usernames and passwords to access data across organizations. FIS bolsters cybersecurity because individuals maintain a single digital identity that is legitimized by a one-stop credentialing.

FIS lets users share information more reliably because each application for access to separate systems represents a point of weakness. When a user has multiple digital identities, cyber criminals have a better chance of attacking at least one of them because it is harder to keep multiple identities safe. FIS also increases government employee mobility because they can log into systems with one digital identity to work remotely.

Government organizations can use FIS for better collaboration with other institutions because participating agencies share agreed-upon standards. They facilitate the authentication process while ensuring appropriate access to important government resources. A common framework from FIS establishes more trust among government institutions and eliminates the pain of setting up separate authentication procedures.

WHO IS DOING IT?

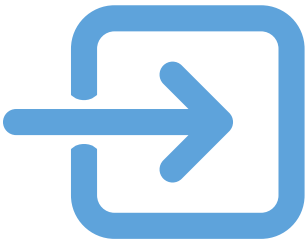
The National Institutes of Health (NIH), part of the Department of Health and Human Services (HHS), is the nation's leading medical research agency. It is also the largest source of funding for medical research in the world, and it provides thousands of high-quality jobs at universities and research institutions globally.

NIH uses FIS to collaborate with colleagues outside its organizations, including those at universities, other HHS departments, operating divisions and other federal agencies. Outside collaborators are authorized through single digital identities by NIH research, grants or administrative groups. They can then use credentials from their organizations to access NIH services.

To create this FIS, NIH partnered with the InCommon Federation as an identity credential provider. InCommon uses Security Assertion Markup Language-based authentication and authorization systems to enable scalable, trusted collaborations among its community of participants. SAML is an open data format for exchanging authentication and authorization data between parties.

As a massive research entity, NIH has extensive partnerships with multiple organizations. FIS is critical to enhancing these collaborations while maintaining cybersecurity. Imagine the lengths NIH would have to go to in order to secure its cyber environment if it had to set up individual identity verification processes with each partner institution and its individual users.

Access to a vast array of NIH resources from so many different institutions implies complexity and difficulty, so coordination is key. FIS has helped NIH better distribute its research while also protecting its information.



Trend #2:

THIRD-PARTY CREDENTIALING

Maintaining a centralized authentication system that a third party verifies to remove the necessity of creating and securing multiple credentials for users

WHY IS IT IMPORTANT?

In 2011, the White House's National Strategy for Trusted Identities in Cyberspace (NSTIC) gave agencies the impetus to use third-party credential providers to validate online users' identities. Similar to FIS, third-party authentication systems enhance cybersecurity by eliminating the need for multiple usernames and passwords.

In this case, a third party verifies the digital identity. Existing credentials are stored in a centralized management system. When a user submits his or her credentials to a new organization, it can use a third-party database to see if the credentials match one of its registered users. If this separate database recognizes the credentials, then the organization will grant the user access. Private sector examples of this arrangement are Spotify or Amazon, which let users log in with a Facebook account instead of requiring new usernames and passwords.

While government has been hesitant to rapidly adopt external identity providers, recent cyberattacks confirm the importance of continuing such efforts.

Third-party credentialing offers government and citizens more choice and confidence when it comes to digital services because they can use credentials from a provider they know and trust. If done well, third-party authentication in government will go a long way in reducing digital barriers for government and citizens, removing identity management costs and efforts for IT teams and the general workforce, and increasing cybersecurity.

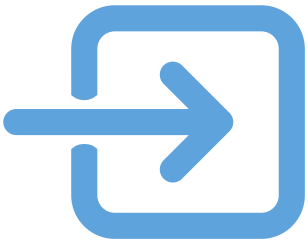
WHO IS USING IT?

Many agencies attempting third-party authentication are using government third parties to verify digital identities. For instance, the Department of Housing and Urban Development's requirement for third-party verification uses reported family annual income and value of assets that a source from the Public Housing Agencies independently verifies. However, this intergovernmental dependence may limit digital mobility for government and create missed opportunities for cybersecurity innovation from the private sector.

The U.S. Postal Service (USPS) is one of the few government organizations that uses private-sector entities for third-party identity authentication. USPS created and maintains the Federal Cloud Credential Exchange (FCCX), a cloud-based hub that acts as a middleman between third-party credential providers and agencies by organizing and managing user information collected from disparate sources. Federal agencies can then leverage those credentials to verify citizens' identities when they access government digital services, instead of requiring them to create new login information.

USPS is pilot testing FCCX. The service operates one of the world's largest computer networks and e-mail systems, handling more than 4 billion communications annually. With so many identities and addresses to protect, the project is an ideal way to develop a credential exchange program that offers the public secure, private, and efficient access to federal government online services.

USPS will use FCCX to make it simpler for individuals to bring their own credentials from an approved external credential service provider so they can log in to federal websites. Other agencies have already started pursuing the pilot project, including the Department of Veteran Affairs (VA), Department of Agriculture, National Institute of Standards and Technology (NIST), and General Services Administration (GSA). By streamlining digital verification, projects such as FCCX will reduce government agency costs, provide better user accessibility, and ensure cybersecurity.



Trend #3:

MULTIFACTOR AUTHENTICATION

Leveraging a security system that requires more than one method of authentication to verify a user's identity

WHY IS IT IMPORTANT?

Although multifactor authentication (MFA) has long been considered a best practice for securing login protocols, many agencies haven't adopted it because of the procedural and technological renovation it requires to implement. However, that is about to change.

After a recent series of data breaches at the Office of Personnel Management (OPM), Federal CIO Tony Scott launched a 30-day cybersecurity sprint, instructing all federal agencies to review and tighten their security measures to prevent cyberattacks. Under the plan, federal agencies have to immediately identify vulnerabilities and quickly adopt MFA provided by the Department of Homeland Security (DHS).

MFA can be achieved by using a combination of at least two of the following factors:

- Something you know, such as a password or personal identification number.
- Something you have, such as a token or smart card.
- Something you are, which involves biometrics, such as a fingerprint.

MFA is necessary to a strong cybersecurity strategy. Without it, any one piece of lost information, such as a password, can endanger an entire system. Requiring at least two difficult-to-obtain processes makes it harder for hackers to access important government information. As a result, multifactor authentication is recognized as one of the most secure methods of verification.

WHO IS DOING IT?

In 2006, the Department of Veterans Affairs (VA) headquarters launched a Personal Identity Verification (PIV) pilot program to meet new security standards and reduce cost. The deployment of cards to more than 200 VA sites nationwide began in mid-2007. Included in VA's MFA protocol is a PIV card checklist and federal government documentation that includes policies essential to the PIV pilot program.

VA promotes the PIV card for its ability to encrypt data, verify users and ensure:

- Confidentiality because only cardholders can read data.
- Integrity by granting cardholders exclusive access to data.
- Authenticity by guaranteeing the origin of the data.
- Non-repudiation by eliminating the possibility of falsified data.

After its data breach, OPM pushed VA to refocus on MFA. Requirements for password authentication languished, but now VA has started implementing more PIV cards to enhance cybersecurity. VA Chief Information Security Officer Stan Lowe issued three memoranda since June 25, 2015, calling for mandatory use of PIV cards for IT personnel with privileged user access and two-factor authentication for all employees accessing the VA network.

Although the policy went into effect July 15, 2015, former VA Secretary Eric Shinseki mandated the use of PIV card credentials as far back as April 2011. Why it took the agency so long to implement this important initiative is unknown. VA, however, is more serious about MFA this year. In the memo, Lowe emphasized, "all local administrative accounts will be disabled unless compliant." The policy also requires all elevated-privilege accounts to be reviewed every quarter and provides for routine spot checks by security officials.

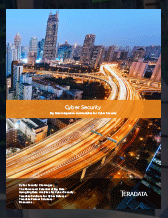
Although implementing two-factor authentication in an agency as large as VA will be a challenge, agency officials are determined to reconfigure and reduce access points and lock down the use of social media from within the VA network.

Data-Driven Cyber Security

Beyond Big Data to Data-Driven Insights

Big data and analytics are becoming some of the most effective defenses against cyber intrusions. Better, faster, actionable security information reduces the critical time from detection to remediation, enabling cyber warfare specialists to proactively defend and protect your network. Teradata delivers a single, authoritative ecosystem integrating information security, cyber security and network operations data, analytics and reporting. Applying deep analytics to integrated security data makes existing defenses more effective and cyber warriors more efficient.

Teradata.com/cybersecurity



Learn more about our approach to data-driven cyber analytics in this informative eBook.

What would you do if you knew?™

TERADATA.

BECOMING MORE SECURE WITH BIG DATA ANALYTICS

An interview with Sam Harris, Director of Enterprise Risk Management at Teradata

It is no longer a given that a network is safe and secure. Security professionals used to be able to sleep at night knowing their networks were virtually impenetrable. But today, adversaries have become more sophisticated, as have their tools and techniques. Motivated hackers will bypass individual security systems and break into your network. It is impossible to keep them out.

To combat those threats, many agencies are increasing the number of security tools they deploy across their network to create a layered defense strategy. While that strategy creates more alerts, Sam Harris of Teradata, a best-in-class analytics solutions provider, said it's actually the wrong way to truly achieve cybersecurity with constrained resources.

"It's a catch-22," Harris said. "[To increase security], you get more tools. But if you have more tools, you get more alerts and many of those are false positives. As you get more alerts, that overwhelms your people, but you can't get more people because there's a shortage. Then you're back at the beginning of your circle of not being secure."

Thankfully, Harris offered an alternative strategy to secure agencies without increasing network complexity or the workload of cyber staff. "Big data analytics is the path out of that conundrum," he said.

Before taking that path, Harris said it's important to understand what true data analytics entails. "Many people will suggest that they are providing analytics when they're really referring to something like summary statistics," he said.

Instead, Teradata defines big data analytics as the ability to compile large and diverse data sets in an integrated fashion, and then apply algorithms to that data to find relationships that aren't evident otherwise. This ability to automatically determine relationships between separate alerts is key to breaking the cycle of increasing alerts without increasing security.

Harris offered an example of how correlated alerts can make sense of the noise: "You may have an alert from your firewall… and then, maybe you receive an alert from your anti-virus software. By itself, it may not look very important, so you decide no action is required. But if you were able to see the alert from the firewall in the context of a simultaneous alert from your anti-virus software, you might think, 'You know what, there's a relationship here.' Seeing the two together changes 'Oh, that's not very interesting to, 'Oh my goodness, this is something that we need to take action on immediately.'"

These correlated alerts provide more information to make quick decisions. "If you can provide more contextual information, the security professional can triage [the alert] more quickly," Harris said. "You're creating an environment where they can actually evaluate more alerts, more quickly in a given work period."

In addition to prioritizing alerts, data analytics can also be used to better detect intrusions within the network. "The game has changed from defending the network to keep people out, to defending the network with the understanding that some adversaries are going to get in," Harris said. "You need to find [attackers] and kick them out before they're able to either ex-filtrate data or damage systems."

Data analytics allows cyber professionals to monitor and compare traffic within the network. This is the key to identifying hackers who have already breached a system.

"Today, [hackers] know how to design their malware to evade the protections from individual systems," explained Harris. "Then they are able to enter your network and move around."

But true analytics can monitor traffic between different tools, comparing activity at the point of entry to other parts of your network. When a mismatch occurs, analysts are alerted to a potential intrusion, even though the hacker initially entered the network undetected.

What's more, this correlated alert is produced without adding new security tools to your infrastructure. "What happens is you actually make old, existing tools more effective," said Harris. That means that cybersecurity professionals have fewer technologies to monitor and maintain, even as they triage more security alerts.

Finally, Harris stressed that these cybersecurity experts don't have to be data scientists to reap the benefits of a data analytics security tool. Teradata's platform "allows data scientists to develop and then push their algorithm into an environment, where security professional can simply pick it up, point it at a data set, and launch it."

"What we're talking about is bringing quantitative capabilities and applying them to the security business problem," concluded Harris. "Big data analytics paired with security professionals can trump the concept of adding new tools that simply produce more alerts and greater false positives."

THE NEW NETWORK

How do you secure a network that spans the globe with limitless endpoints and millions of users? That's the question every cybersecurity professional in government is trying to answer as information systems connect to new people, places, and devices at an unprecedented rate.

Unfortunately, there is no one solution to this challenge. Instead, organizations will have to deploy a multifaceted approach to securing the new network, which will require multilayered security not only using traditional tools, but also "things" and mobile devices.

4

5

6

Trend #4:

MULTILAYERED SECURITY

Layering security tools and technologies to create a dynamic environment of first, secondary, and tertiary cybersecurity protocols

WHY IS IT IMPORTANT?

With each passing year, it seems we hear another motto about how we should protect our critical information. One year, the common wisdom for agencies was securing the perimeter. The next, administrators were told to create "defense in depth." Then network segmentation was the golden rule of protection.

None of these tactics is wrong, but no single strategy is enough. Instead, a combination or layering of these tactics is integral to creating a holistically secure environment. Why can't you have just one?

Consider a malware attack. Your firewall might block the hack from entering your system. But what if it doesn't because the packet is so well disguised? You'll want another layer of internal defense that might prevent it from reaching the information target or end user within that system. If that fails, too, you'll want yet another layer of defense in place to make sure that once the attack is launched, it doesn't gain access to everything on your system.

In such a scenario — an unfortunately common one for agencies today — multilayered defense is necessary to maximally secure your networks. It provides a strong defense to prevent hacks but, more importantly, it provides contingency for when things go wrong.

WHO IS DOING IT?

Perhaps the best example of multilayered defense is DHS' intrusion detection system, called EINSTEIN. In some aspects, the system can be seen as a single layer of perimeter defense. EINSTEIN's overarching mission is to monitor and detect potentially malicious traffic at the system's entry point.

Yet like cyberthreats, this defense system has evolved to become more complex and provide additional levels of security. DHS deployed the first iteration, EINSTEIN 1, in 2004. It performed basic intrusion monitoring by analyzing activity entering and exiting agency networks. Launched in 2008, EINSTEIN 2 enriched that capability to detect and alert agencies to known or suspected cyberthreats when they cross the "fence" to a government network.

The third iteration, called EINSTEIN 3 Accelerated (E3A), extends the system's protection by delivering intrusion prevention capabilities to the Internet service providers that work with federal agencies. This most recent version can execute near-real-time deep-packet inspection of traffic before it enters and after it exits government networks.

When it was deployed in 2013, E3A covered only about 45 percent of agencies. However, on July 8, 2015, DHS Secretary Jeh Johnson announced that this latest iteration of the intrusion detection system would be deployed across all federal civilian agencies by the end of this year. According to Johnson, "Since its introduction, E3A has blocked more than 550,000 requests to access potentially malicious websites." Now he wants to extend that defense across the entire enterprise.

Finally, to truly cover federal agencies with multilayered protection at the perimeter and inside the network, EINSTEIN will work in concert with another DHS program: Continuous Diagnostic and Mitigation (CDM). At the same time that Johnson announced the extension of E3A, he also mandated the extension of CDM, which monitors agency networks internally. Together, CDM and E3A will provide true multilayered protection across federal agencies.

Trend #5:

CITIZEN MOBILITY PROTECTED

Ensuring government digital services can be accessed anywhere, on any device, without risking information security

WHY IS IT IMPORTANT?

Mobility has been a hot topic for government IT for several years. Because of that, NIST has worked diligently to create mobile security standards for enterprise solutions — that is, solutions that can be deployed agencywide — while organizations like the Defense Department are launching their own bring-your-own-device programs to keep personnel mobile but secure. Now, the focus is on extending that mobility to citizens.

Citizens increasingly expect the same convenience of access to government services as they get from the private sector. In fact, mobile-only Internet users outnumber desktop-only users today. As a result, more government organizations are seeking ways to facilitate access to their digital services from any mobile device.

This effort comes with new challenges to security, however. As part of its Making Mobile Gov Project, GSA surveyed several federal agencies to understand their biggest barriers to mobile security. Three common concerns surfaced:

- Government IT security teams need more understanding of the risks associated with mobile products to better manage them.
- Agencies need to develop security standards for all device platforms.
- New security protocols need to be considered for mobile projects that collect new datasets.

In other words, agencies must be prepared to deal with every device that can access their network, rather than just those authorized for workers' use. What's more, these security considerations must be integrated into every mobile project before they are developed and opened to the public.

WHO IS DOING IT?

Recognizing the need to secure mobile digital services, the Federal CIO Council formed a Mobile Technology Tiger Team (MTTT) to create a common set of criteria for vetting mobile application software. After a year and a half of development, the group released this standard set of security procedures and expectations in November 2014.

The criteria follow the example of NIST's Special Publication (SP) 800-163, "Vetting the Security of Mobile Applications." However, SP 800-163 mainly focuses on securing a mobile workforce while MTTT's criteria extend to any government application, including public-facing services.

These new criteria provide two significant efficiencies for agencies. First, MTTT's effort eliminates the potential redundancies resulting from individual agencies' development of their own criteria for mobile projects. This saves IT professionals both time and money, because they can incorporate trusted standards without investing in their own cybersecurity research and development.

Second, a governmentwide vetting standard enables agencies to partner with third-party mobile vendors and establishes a mutual understanding of exactly what security measures should be incorporated into mobile projects.

Two agencies, DHS and DoD, have already pledged to implement MTTT's recommendations in future projects. The Defense Information Systems Agency also added a special annex in May 2015 to accommodate specific DoD security and mission requirements. Other agencies can access the criteria and DoD annex through the National Information Assurance Partnership.

To encourage industry adoption, the CIO Council planned a series of industry education days to generate awareness and understanding of the criteria.

Trend #6:

THE SECURITY OF THINGS

Deploying cybersecurity tactics and technology to secure Internet-connected physical systems

WHY IS IT IMPORTANT?

You've probably heard of the Internet of Things (IoT), a phrase that describes the networked connection of physical devices, systems, and tools to one another and the Internet. As we explain in our recent guide, What the Internet of Things Means for the Public Sector, these connected devices are changing the way we live and govern. Data collected from connected sensors can inform decisions or even trigger automated chain reactions to drastically improve emergency response, infrastructure management, and a variety of other public sector responsibilities.

Yet even as IoT creates new possibilities for government, it also creates new cyber vulnerabilities. When you connect a car, building, or device to the Internet, you also connect it to your network, creating a new endpoint for hackers to attack.

In many instances, the fallout from a breach of a physical system can be even scarier than an information system hack. Consider the potential damage a hijacked car or nuclear stockpile could cause. Now we see the discussion moving beyond the Internet of Things to consider how to maintain the "Security of Things."

WHO IS DOING IT?

The Virginia Cyber Security Commission was launched in 2014 to tackle a number of traditional state cyber concerns including workforce training, network security, and industry partnership. This year, the commission is expanding its scope to a new area of cybersecurity: cars.

The commission created a public/private working group in conjunction with the Virginia State Police. Gov. Terry McAuliffe explained why: "High-tech systems now used in most automobiles are opening up potential new avenues for cyberattacks. We have the opportunity to lead the nation in the establishment of safeguards protecting the vehicles of Virginia's 5.8 million licensed drivers."

The group is working directly with law enforcement to identify vulnerabilities in Internet-connected vehicles in hopes of improving the cybersecurity of all automobiles and drivers within the state. It has three goals:

- Identifying low-cost technology to help law enforcement determine when vehicles are hacked.
- Developing strategies for citizens and public-safety personnel to identify and prevent threats to connected devices and vehicles.
- Exploring economic development opportunities related to this specialized, physical-system cybersecurity field.

Ultimately the commission will develop tactics in collaboration with law enforcement and the private sector that can secure IoT within the state.

TANIUM™

With Tanium you can answer critical questions about the current state of your endpoints & take immediate action as needed. Across all of your systems globally.
All within 15 seconds.

ASK
your question in plain English

KNOW IN 15 SECONDS
what is happening across all of your endpoints

- How many laptops are missing critical security patches?
- How many unmanaged machines are on my network?
- What versions of Java are out of date in my environment?

ACT
change all impacted endpoints as needed

15-Second Visibility & Control Over Every Endpoint. Even Across the Largest Networks.

Impossible? Think again.

Let us show you the magic of Tanium.

Learn more at www.tanium.com

GIVING THE FEDERAL GOVERNMENT VISIBILITY AND CONTROL

An interview with Ralph Kahn, Vice President of Federal at Tanium

These days, getting hacked is not a matter of "if" – it is a matter of "when". It is therefore increasingly important to have tools that provide visibility into what is happening on your endpoints in real-time in order to minimize the potential damage.

To discuss how the public sector can truly protect itself, we sat down with Ralph Kahn, Vice President of Federal for Tanium. Tanium is a next generation endpoint security and management firm that gives agencies visibility and control over every endpoint in just seconds. The firm also helps improve government quickly identify indicators of compromise (IOCs) and subsequently take the appropriate actions to minimize any damage.

Kahn touched on the recent OPM hack that compromised the personal information of more than 21 million federal employees. Part of the reason this occurred, according to Kahn, is that the government is working with older legacy technologies that are unable to protect against the ever-changing threat landscape.

"The government has thousands and thousands of applications out there that have been developed without the ability to incorporate newer security controls," he said. "Unfortunately, it would be prohibitively expensive and time-consuming to replace them all. A more effective approach would be to look at our infrastructure, make the assumption that we're going get hacked anyway, and then focus on being able to detect and remediate threats and intrusions much more quickly than we do today."

Kahn also noted that even agencies with the most sophisticated and effective cyber defenses are susceptible to hacking by advanced and relentless opponents.

"The U.S. government has a lot of very sophisticated enemies trying to get at its information," he said. "If the government truly wants to prevent something like the OPM breach from happening again, the focus needs to be on remediation. Agencies must have a much faster way to see what's going on in their environment, and a much faster way to react when they see something inappropriate happening."

This is where Tanium can help by minimizing potential damage resulting from successful attacks. Today, many network technologies provide a lot of data about what is transpiring on your network and what data is moving across your network boundaries, Kahn explained. The problem is that hackers are aware of this, thus they encrypt their attacks or hide data in other ways to make network technologies much less effective at catching them.

What organizations really need are tools that monitor data on the endpoint in real-time, then see which databases and data files are being accessed, and then look for patterns of behavior that are inappropriate.

"What our technology can do is look for IOCs that might already exist, and then correlate that with the data that you get from the network to get a holistic view of what's going on in your IT enterprise," Kahn said. "Tanium allows you to do that on the endpoint, by giving you the ability to query any information you need in 15 seconds across all your endpoints at scale. It doesn't matter if you have a thousand or a million endpoints – Tanium can give you that information."

At one large government customer, Tanium scanned over 150,000 endpoints for the presence of IOCs in less than 3 minutes. When IOCs were found, Tanium was able to automatically respond in seconds. This ability to detect IOCs and automate a response allows agencies to fight the intruders on a more level playing field for the first time. Automated detection of known threats also frees up cyber analysts to hunt for new intruders in the enterprise, further increasing cybersecurity.

Kahn explained that Tanium's approach gives you a 360-degree view of your network in real time. "What's important about that," he said, "is that it gives your smart people the ability to make really good decisions. When you have good data and good tools, you can use them to make much better decisions about how to protect yourself."

"Tanium's hallmarks are three things: speed, scale and simplicity." Kahn added: "The speed? We can get any data that you need off your endpoints in less than 15 seconds. Scale? We can provide that for up to millions of endpoints. And simplicity — the people who use our tools do it with a Google-like interface. You don't have to be a rocket scientist to participate in cyber defense. You just have to know a little bit about your subject matter, and have the right tools. If you provide the people, we'll provide the tools, and you can protect your data."

Interview

MOBILITY AND INFORMATION ENTERPRISE AT THE MARINE CORPS

An Interview with Rob Anderson, Strategic Technical Advisor to the Director of Headquarters Marine Corps Command, Control, Communications and Computers

The Marine Corps has been working on mobilizing its information enterprise since 2013. Rob Anderson, Strategic Technical Advisory to the Director of HQMC C4, has been an integral member in the development of the Marine Corps Mobile Information Enterprise Strategy (MCIENT). MCIENT is the foundation of the Marine Corps Cloud Private Computing Strategy and the Marine Corps Commercial Mobile Device Stratey which promote system and application interoperability, information access, data exchange, domain security, single point authentication, IT service management capabilities, and integration of mobile capabilities to create a more efficient workforce. Anderson said the MCIENT is the foundation of command, control, communications, and computers capabilities.

In his position, Anderson interfaces with partners across the department, federal government, and private sector. "I try to leverage people's really great ideas to create sound strategies," Dr. Anderson said. "I also interface with our industry partners quite a bit. I keep pace with what they're involved with as well as their business."

In an interview with GovLoop, Anderson explained how USMC is leveraging the MCIENT strategy to enhance workforce mobility for warfighters while maintaining cybersecurity.

MOVING DATA TO THE EDGE

A key objective of the MCIENT is moving data forward, or out to the edge, to support forward deployed forces with the data they need to take action. Moving data to the edge means making data accessible outside the office, to deployed Marines and Sailors. "For us, we need to get that data as far forward as possible, so we can input any data we discover about known bad actors into multiple databases that reside within the government," he said.

For instance, some solutions acquired under MCIENT enable deployed Marines to make bad actor data widely accessible. "There are known bad actor libraries that are accessible to warfighters, which allow our forces to gain access from the edge. The goal is to allow them to access this data are a checkpoint or on patrol via a commercial mobile device," said Anderson. Those Marines can scan the identities of individuals using a biometric scanning device and ad them to a database. If the individual pops up in the program as a known bad actor, the Marines will be able to act accordingly.

"This is the power of moving data as far forward as possible," said Anderson. "It doesn't have to be Marine Corps data. It needs to be data that is relevant to the mission and geographical area where Marines are operating."

MOBILITY AS A SERVICE

Currently only six percent of the Marine Corps have a government furnished mobile device. So, Anderson and his team at HQMC and SPAWAR Atlantic developed a concept called, "mobility as a service."

"That's where you have an industry partner, who's in a cloud-based FedRAMP facility, providing an enterprise mobility management portal that would manage a container that resides upon our device," Anderson said. "That container can be a government furnished device or a personal device that meets certain security requirements."

One problem in implementing mobile device security is the tendency to be too device-focused in security efforts. "We have firewalls and security software on our laptops and our desktops. We have security guides pertaining to devices as well as those that protect the server. But that's all focused on the equipment," Anderson said.

He suggested the focus should be more data security-based. "If we can maintain the integrity of the data as it's in transit and at rest, it really doesn't matter where it sits because that data is safe." He added, "Once you mediate those vulnerabilities, you figure out how to solve a particular problem."

Anderson made the following suggestions for stronger security-based strategies for mobilizing information enterprise:

- ***Integrate cyber strategies early on.*** When planning and conducting the first stages for information enterprise mobility, integrate cybersecurity principles from the beginning. Anderson said, "The cybersecurity element, or the information assurance piece of the technical solution, is baked into the problem. Therefore, when we go into the accreditation process, we go in knowing what to test and validate."

  Early integration of cybersecurity principles allows for targeted penetration testing and enables your agency to report industry software that does not meet certain security requirements.

- ***Talk to industry partners.*** Outside actors and vendors are key to implementing strong cybersecurity software and strategies. Anderson stressed the importance of meeting with and talking to industry partners regularly. "That's the only way we evolved our commercial mobile device strategy to the state it's in today," he said. "Take the time out of your schedule to talk to your industry partner. Sit down with your counterparts, read their strategies, go talk to their CIO and CTO, and find out how they're solving problems."

  Private sector collaboration is key to cyber-secure strategies, especially within the mobile information enterprise. Incorporating outside expertise and insight helps develop stronger strategies, ideas, concepts, and products that government agencies may lack.

- ***Have Patience.*** Anderson's final advice was not to rush a cyber-secure mobile information enterprise. "Having patience when working in the federal space is required," he said. It is important to make sure you address everyone's security concerns, because the last thing anyone wants is a government employee jeopardizing his security or the safety of the organization.

Here's an idea: Put the cloud inside a printer.

The world's most preferred printers.

New HP JetAdvantage Private Print.[1]
Cuts printing costs, keeps documents secure.

Think of them as the printers with the cloud inside. The all-new HP LaserJets come with JetAdvantage Workflow Solutions built in. Save time, toner, and paper by eliminating abandoned or misplaced print jobs. Protect your printing environment, manage your users, and print more efficiently. All at no extra cost. See them at work at **hp.com/go/newlaserjets**

The world's most preferred printers: Worldwide printer market share, and HP printer brand awareness, consideration, and preference study in 9 markets 2014.
[1]HP JetAdvantage Private Print is available only in North America and select European countries on many HP printers and MFPs. Feature is available at no charge and requires the printer be connected to the Internet with web services enabled. Card reader is available for separate purchase for selected HP devices with touchscreens. For more information and device compatibility details, see hpjetadvantage.com

ARE YOU OVERLOOKING PRINT SECURITY?

An interview with Michael Howard, Security Practice Manager and Business Development at HP

In today's connected world, cybersecurity is far more than keeping malicious applications off your smartphone or thwarting attacks before they wreak havoc on your computer systems. It seems just about anything can — and is — being connected to the Internet these days, and with that increased level of connectivity comes an increased level of risk.

Even vending machines are being hooked up to the Internet. And that's just another endpoint through which hackers can worm their way into your networks, if those connections are not secured, maintained and monitored. As more and more devices and assets come online, there's one in particular that many organizations have overlooked, said Michael Howard, Security Practice Manager and Business Development at HP.

"One of the things that a lot of customers do today is they'll secure their entire IT infrastructure, but they'll exclude printers," Howard said. "Print has been one of the largest oversights in IT areas."

How can the problem be solved? Education is key.

When leaders don't understand the significance of an investment it's likely to be cut rather than grown. The harm there is that security investments fall by the wayside until there's an incident, and it's too late.

"At HP we have been building our security portfolio around print and providing education, as well as security advisory services. This is where we go in and help customers understand the need for securing printers at the same level as the rest of their IT," Howard explained.

HP is making large investments in developing print security solutions, including hiring more experts who are credentialed and well-equipped to help agencies sort out print security needs.

The ultimate goal for agencies is to ensure that every endpoint on the network, including printers, have a security policy and ensure that policy is implemented and regularly updated. That's especially true now that printers are moving under the purview of IT departments, as opposed to facilities departments.

"What we like to tell customers, quite simply, is if it touches your network, it needs to be treated as a equal citizen when it comes to security," said Howard, who manages HP's worldwide team for the security practice around print.

Howard stressed that agencies cannot afford to set policies and fail to review and update them regularly. At a bare minimum, organizations should be reviewing their security policies every three months, Howard noted. "It is something that has to be proactive," he stressed.

So where does an agency start with print security? What policies should agencies enforce to secure their printers, many of which are far more sophisticated than the ones developed decades ago?

Jason O'Keeffe, Security Solution Expert for the America's Region at HP, offered these best practices:

- Enforce encryption and security monitoring. Printers store sensitive information, and that data needs to be protected. If a printer is out of compliance with encryption standards, the issue should be reported to the security team and addressed.
- Establish policies for securing built-in firewalls. Some printers come with their own firewalls that must be managed through policies.
- Check the settings. Every network device — server, storage, computer or printers — by default will have unsecure protocols. So you have to ensure that the unsecure settings are changed and brought into line with your organization's policies.
- Secure embedded web services. Printers have embedded web services, and every web server that supports those services should be properly secured.

"Printers are not very different from any other network device on the environment," O'Keeffe said. Policies that govern the security of printers should also be monitored and reported regularly. This is especially true if your agency is undergoing major IT changes or upgrades.

"If you undergo a major upgrade, it's important that you keep an eye on existing controls and constantly monitor them," O'Keeffe said. That way you can ensure security features aren't altered or completely changed.

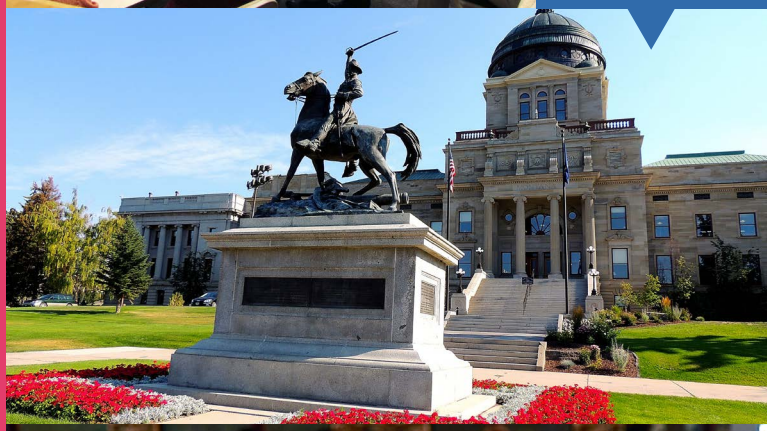
In addition to helping agencies set print security policies, HP and its team of experts is also looking ahead at future capabilities that will boost security. Additionally, HP is developing solutions that provide built-in security tools for printers, similar to what's already available for desktop and laptop computers.

"We are building a lot more security policies and security solutions into the devices themselves, so that you're starting with a very secure device and you can start layering solutions on top of that," Howard said.

THE RETURN OF THE HUMAN

The notion that advanced technology alone can thwart cyberthreats has been discarded. With each new successful hack, it becomes clearer that you cannot execute or counter an attack without considering the human element. Many hacks, including malware and phishing attacks, directly target weaknesses in the human, rather than technology, chain. And as we combat threats, hackers engineer new countermoves to evade our protections. In 2015, the human has returned to take center stage in the fight for cybersecurity.

7



8

9

Trend #7:

CYBER AS EVERYONE'S JOB

Empowering every system user, not only the IT team, to detect and protect against cyberthreats

WHY IS IT IMPORTANT?

When asked during a congressional hearing who was responsible for the 2014-15 OPM hacks, former Director Katherine Archuleta responded, "This is an enterprise-wide problem and cybersecurity is the responsibility of all of us."

Although it appears that the OPM breach resulted from an exploitation of a system vulnerability, Archuleta's point was clear. We can no longer rely on one person or department to protect government information systems, because security is everyone's job.

What's more, she's not the only government leader who thinks that. According to one survey, more than half of government IT professionals identified careless or untrained employees as their biggest security concern. That's unsurprising when you consider that many hacks directly target untrained employees — the ones through whom it's easier to gather credentials and infiltrate information systems. Furthermore, the unintentional loss or exposure of documents can be just as damaging to an agency as any intentional insider breach.

Agencies have a substantial opportunity to buffer cybersecurity simply by educating all their employees — not just IT professionals — to better handle sensitive information.

WHO IS DOING IT?

Starting in fall 2013, Montana officials mandated annual cybersecurity training for all state executive employees. To provide that training, the Information Security Bureau (ISB) partnered with the SANS Institute, a provider of security training and certification. The resultant program, called Securing the Human, is a compilation of online cybersecurity courses that all state government employees can access.

Training programs are broken into three categories: general awareness, technical, and management. Each program correlates to an employee's role and level of technical skill, with more senior employees having to take both basic and advanced instruction.

General training is required for every executive branch employee and covers basic cyber hygiene best practices, including Internet security, password protection, mobile device security, and privacy maintenance. Technical training offers more advanced skills such as encryption and cloud computing instruction. Finally, management training offers leadership guidance and lessons on red flag alerts within security systems.

In addition to these three programs, which total about five hours and cover more than 25 topics, employees may access additional training relevant to their specific job functions. The program is mandatory for all executive branch staff, but other employees and state contractors may also participate in training programs at no cost.

To extend cybersecurity training beyond the online classes, ISB also provides reference materials, monthly security newsletters, and tips of the week to continue employee education. The State Information Systems Security Office also promotes cybersecurity awareness with events, games, posters, and prizes during annual Cybersecurity Awareness Month.

Trend #8:

BEHAVIORS AS INDICATORS

Analyzing human patterns of behavior to detect and counter insider threats before they harm an organization or expose sensitive information

WHY IS IT IMPORTANT?

Training a person to better protect agency information systems is one important way to address behavior-based threats to security. However, that's only one piece of the insider threat puzzle. Although most public sector employees are part of the solution to insider threats, others intentionally expose agency information and become the problem itself.

To combat those malicious insiders, the human element of a hack is by far the most important. What motivates people to expose sensitive information and how they do it are two people-specific identifiers that must be considered in order to detect insider threats before they occur. When an insider threat is successful, agency officials must learn exactly how and why that breach occurred so it won't happen again.

Of course, malicious insider threats are rare. They represent anomalies in public servants' behavior. That's why it is all the more important to understand what normal behavior for an employee is and what deviations from that pattern might signify a problem. Only by targeting the human element of an insider threat can we effectively protect our cyber systems.

WHO IS DOING IT?

The Defense Advanced Research Projects Agency (DARPA) partnered with the Georgia Tech Research Institute to create a program called Anomaly Detection at Multiple Scales (ADAMS), which can scan massive amounts of disparate data using a series of complex algorithms. But don't be fooled. Just because the team is working with data and equations doesn't mean that humans aren't at the very heart of this project.

In fact, this program is meant to examine huge amounts of human-generated data, including e-mail communications, text messages, file transfers, and even keystrokes, to determine what behavioral patterns preceded insider threats in the past. Based on their conclusions, the program will then create algorithms to identify those same behavioral patterns in current government systems. According to DARPA, these algorithms could predict "a soldier in good mental health becoming homicidal or suicidal," an "innocent insider becoming malicious," or "a government employee [who] abuses access privileges to share classified information."

By targeting common human indicators of a potential intentional or inadvertent insider threat, the program can automatically direct security personnel to events before they occur. "Our goal is to develop a system that will provide analysts for the first time a very short, ranked list of unexplained events that should be further investigated," explained one investigator from Georgia Tech.

Although Georgia Tech is a primary partner, several other academic institutions and the Science Applications International Corporation (SAIC) are also contributing to the $35 million project. While it began in 2011, ADAMScontinues today and incorporates new data sources as successful insider threats such as the Pfc. Bradley Manning leak occur.

Trend #9:

BUILDING A NEW SECURITY TEAM

Doubling down on efforts to attract or train personnel to become the next generation of cybersecurity professionals

WHY IS IT IMPORTANT?

It doesn't matter how many robust security solutions you have in your IT environment if there are no personnel to use and react to them. Even automated solutions require individuals to install and maintain them.

That's why the government has dedicated significant resources to hiring and training cybersecurity personnel across branches and levels of government. But government officials are not the only ones realizing the importance of having trained cybersecurity staff to back trusted solutions. Private industry is proving a fierce competitor in the market for top cyber talent, and government, with fewer resources and benefits, often loses the fight. For instance, even with new incentives from defense chiefs, U.S. Cyber Command is struggling to reach its target of 6,000 security personnel by 2016.

So how do we hire the best of the best cyber warriors to defend government? Some organizations believe a complete overhaul of the civil and military services is required to make benefits more appealing to cyber professionals. However, other agencies, particularly at the state and local levels, are taking more immediate steps to beef up security personnel.

WHO IS DOING IT?

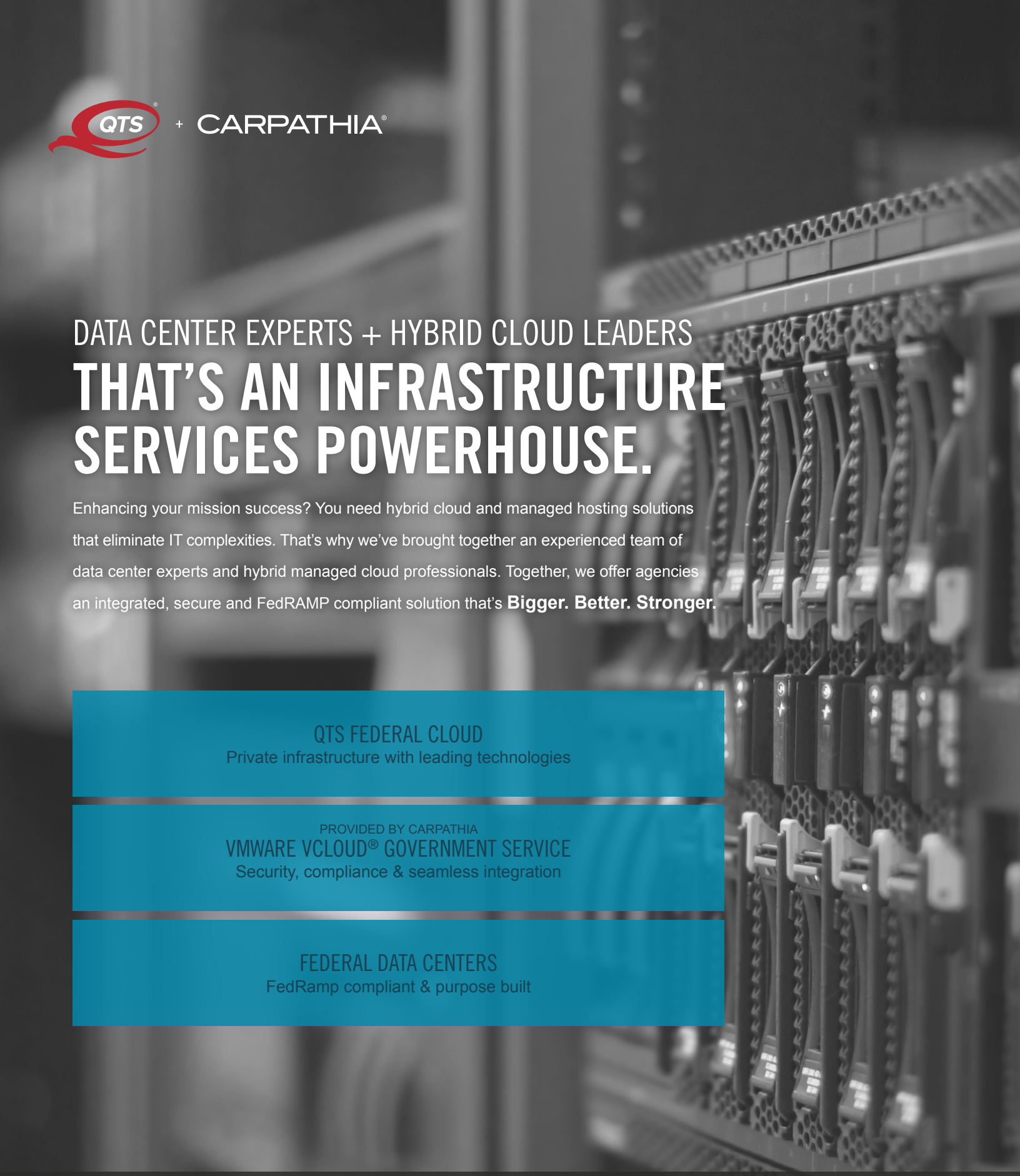
Texas is one such example. Officials at the state's Department of Information Resources (DIR) decided that instead of hiring cybersecurity professionals, they would train existing IT talent to get them directly involved in state cyber efforts.

Launched in 2014, the Texas InfoSec Academy offers current state IT and security professionals the ability to train specifically in cybersecurity. Right now, this training is limited to state information security officers and chief information security officers, but DIR officials hope to extend the program to all IT employees soon.

The program offers six career tracks that span cyber issues: Information Systems Management Leadership, Incident Handling, Forensics, Disaster Recovery, Application & Secure Code, and Penetration Testing & Hacking. It also offers several certifications. The entire curriculum leverages information provided through DHS' National Initiative for Cybersecurity Careers and Studies and is presented in weekly classes that are primarily computer-based.

One large benefit of this program is that it transitions employees who are already invested in public service into the cybersecurity field, thereby overcoming the hurdle of initially drawing talent into government. It also decreases hiring costs by training people who are already employed by the state.

The program is also open to higher education institutions in the state in hopes that young IT professionals will be attracted to public service and cybersecurity through the training. As of April 2015, 82 organizations had 175 students enrolled in the academy.



QTS + CARPATHIA®

DATA CENTER EXPERTS + HYBRID CLOUD LEADERS

THAT'S AN INFRASTRUCTURE SERVICES POWERHOUSE.

Enhancing your mission success? You need hybrid cloud and managed hosting solutions that eliminate IT complexities. That's why we've brought together an experienced team of data center experts and hybrid managed cloud professionals. Together, we offer agencies an integrated, secure and FedRAMP compliant solution that's **Bigger. Better. Stronger.**

QTS FEDERAL CLOUD
Private infrastructure with leading technologies

PROVIDED BY CARPATHIA
VMWARE VCLOUD® GOVERNMENT SERVICE
Security, compliance & seamless integration

FEDERAL DATA CENTERS
FedRamp compliant & purpose built

What's driving cloud security technology purchases?
Get the free 451 Research report here:
QTSDataCenters.com/Security-Whitepaper

LEARN MORE AT
QTSDATACENTERS.COM/CONTACT
OR CALL 1.877.QTS.DATA

CRAFTING EFFECTIVE CYBER PARTNERSHIPS, ONE AGENCY AT A TIME

An interview with John Lind, Vice President of Federal Sales, and Oliver Schmidt, Chief Audit Executive at QTS Data Centers

Four years ago, the White House unveiled the Cloud First policy. The White House mandated that agencies must evaluate safe, secure cloud computing options before making any new investments. It sounds easy enough, but many agencies balked. There was a real fear for many that moving to the cloud would leave agencies vulnerable to increased cyberattacks.

In order to help agencies evaluate the risks associated with moving to the cloud, the Office of Management and Budget crafted and updated two security compliance measures FISMA and FedRAMP.

While these compliance measures are a good first step, in order for agencies to be fully secure when moving to the cloud, they need to focus on more than just checking the compliance boxes.

GovLoop sat down with John Lind and Oliver Schmidt from QTS, a data center provider, to learn about how compliance does not equal security. "We try to get across to agencies that as the cloud service provider we have gone through all the compliance requirements including FedRAMP, FISMA," said Lind. "Relying on commercial cloud service providers like us, they're in better shape and get better services than if they try to do it themselves."

One of the reasons cloud environments are more secure, said Lind, is because many agencies' current architectures and systems are outdated. "The reason we're in business is to provide high-level quality security services so agencies can focus on their mission and not worry about security. Our highly qualified staff utilizes our compliant data centers combined with best of breed hardware and software to create, operate and maintain premium services. That's our business. That allows Government IT directors to be able to focus on their top priorities – their mission and programs - and let us handle the security requirements."

However, just because cloud providers can take on the security burden for agencies, it doesn't mean that agencies lose control over their data. Compliance doesn't equal security. True security comes from implementing best practices from industry and government. Oliver Schmidt of QTS explained: "I think a lot of fear with moving to the cloud comes from feeling like you have to relinquish control. We're not looking for agency IT staffs to relinquish control. We want to enter into a partnership."

The partnership allows agencies to move away from a check box-style security. "Agencies really need to pick cloud providers that are more than just FedRAMP certified. For example, an agency may need certain managed services. The agency should target a cloud service provider that offers additional managed security services and meets multiple compliance certifications, like ours," said Lind.

While relying solely on compliances or mandates to remain secure is ill advised, agencies do need to remain compliant with federal regulations. Those regulations can and should be embedded into the cloud process from the beginning. "Take healthcare for example, a hospital doesn't just have to think about tech requirements like FISMA, but also compliance standards like HIPPA. We create multiple compliance to assure that there are no gaps," said Schmidt.

The cost of staying compliant is also a major factor. "By going with a provider that's doing compliance for multiple agencies and sectors, we can definitely make it more efficient in terms of attaining those compliance banners because we can leverage best practices across fields," explained Schmidt.

"Every day we are working with differing compliance regulations and control frameworks from the federal government's NIST Special Publication 800-53, to the Control Objectives for Information and Related Technology (COBIT) for business, Payment Card Industry Data Security Standards, and the American Institute of Public Accountants Service Organization Control reports. Each of those frameworks and standards focus on different aspects of security and compliance," explained Schmidt. "The advantage for any of the federal agencies that are working with us is, they'll get to hear about some of the things that we're seeing within the other standards that may be of interest to them beyond their own compliance standard."

Additionally, each individual program within an agency might have different requirements. Agencies do not want to approach multiple vendors for each system. "They want a provider that can demonstrate capabilities in handling lower level classified information systems within for example a federal community cloud, provide them with hybrid cloud capabilities that can interact with existing systems, and/or for more classified systems with a dedicated private cloud," said Schmidt. "We are able to demonstrate our capabilities very well in that area."

In the end, moving to the cloud shouldn't be frightening for agencies if they create a fully secure IT environment and partner with industry to leverage security expertise and resources.

Interview

SECURING CYBER ENVIRONMENTS THROUGH THE WORKFORCE

An interview with Barry Condrey, Chief Information Officer for Chesterfield County, Virginia

A common misconception is that cyber criminals only target systems. In reality, these criminals target employees to get access to government systems and citizen data. Chesterfield County CIO Barry Condrey says that's why cybersecurity is not just about sophisticated technology, but also about leveraging your workforce to help create a secure environment.

"Something we constantly reinforce with our employees is that they are the target," Condrey said. "Employers need to begin putting cyber language in job descriptions for a wide variety of people. We consider contractors, kitchen staff, code developers, vendors, and vendor employees all as part of our cyber workforce."

DANGEROUS ASSUMPTIONS

With increased dependence on technology comes an increased need for awareness in the cyber workforce, especially of dangerous assumptions that can affect an entire organization's information security program.

Assumption 1: The more IT skills a person has, the less you have to worry about securing the environment.

This stereotype promotes the idea that IT people intuitively know what to do in the event of a breach. Although they may be more knowledgeable in such circumstances, organizations should not solely depend on IT personnel.

Take database administrators, for example. "They're an example of a group that really does need extra cyber training as well as mitigation strategies," he said. It's important to ensure that the general workforce is well trained in order to avoid the moral hazard of overdependence on tech staff.

Assumption 2: More money means more security.

Some leaders assume that by spending a lot of money on equipment and new technology, they will create a high-security environment. However, given the ever-increasing complexity in cyber-threats, Condrey said, we can't rely on technology alone to keep pace. "It's really the human element and it's how well you've used the equipment that will reduce your risk profile," he said.

Assumption 3: Millennials leak the most information.

"You've probably heard the stereotype of millennials being leaky because they're so plugged in. We find that to be just the opposite. We find a lot of millennials are very focused on their information security. They know how plugged in they are and they seem to know what the risks are," Condrey said.

The reality is that baby boomers approach technology differently than younger generations. Since they know they understand technology a bit less, baby boomers are usually stronger proponents of information security, which creates the illusion that millennials are less concerned with securing information.

Assumption 4: Organization leaders don't like security.

The reality is leaders of organizations would rather be prepared for the worst. "People assume chief financial officers, chief executive officers, county administrators, city administrators, and other agency heads don't want to deal with it," Condrey said. "My experience is that CFOs and people in leadership don't like surprises." In short, don't be afraid to communicate details of any information security problems to higher-ups.

Assumption 5: Some organizations don't have information worth stealing.

Any government organization has information worth stealing, even if everything is public and shared with citizens. "Even if you don't think you've got information worth stealing, you have the public trust. You have a certain degree of responsibility, no matter what your position or your line of business within the organization, to keep information secure," Condrey said. No matter how transparent the organization, information is always vulnerable.

ENGAGING A CYBER WORKFORCE

In addition to debunking workforce myths, Condrey shared his insights based on workforce challenges within Chesterfield County's cyber environment. Engaging a government workforce is critical to ensuring security, especially as cybersecurity workforces shrink every year and new technologies emerge. Condrey described this as "a breeding ground for security risk." Motivating your workforce to be engaged in cybersecurity is one of the most important precautions you can take.

"The overworked, distracted, and disengaged employees are inherently going to make more mistakes with information security," Condrey said. Dealing with cybersecurity requires attending to employee morale as much as attending to technological systems. "If you don't think your job matters to the organization, how engaged are you going to be with information security?" he asked.

Low morale leads to the most damaging factor to organization information security — the "Great Copout," as Condrey referred to it. "That's where we see employees in organizations saying things like 'There's no money, leaders don't listen and we just have what we have,'" he said. This attitude affects system productivity, effectiveness, and efficiency as well as information security. "Don't hide behind the things you can't control. Illuminate them."

Condrey recommended the following tips to ensure a more secure cyber workforce. He emphasized that it starts with a culture change. "Take every opportunity to have a conversation about cybersecurity," he said.

- Include information security in minutes: "An educated, informed, and motivated employee is your single best weapon in the fight for information security," Condrey said. Insert points on relevant information security in meeting minutes, newsletters, trainings, and employee orientations. Make sure new employees understand the importance of information security, subsequent policies, and their responsibilities.

- Encourage friendly competition: Condrey and his team regularly hold contests to challenge employee knowledge about information security. This can be done through poster contests, e-mail blasts, and intranet sites. It's a great way to boost employee morale while enhancing cybersecurity awareness.

- Change delivery methods: "If you simply put guides in front of people and have them read a 12-page policy, answer three questions, and certify them for the next five years, that's not doing anybody any good," Condrey said. He recommends training for cybersecurity that fits the devices and job responsibilities of the employee. He often uses the "Securing the Human Series" videos by the SANS Institute for training county workers.

- Incorporate mitigation strategies: "All information security programmers need to recognize when the risk is too high and what to do about it. Mitigation strategies are always needed," Condrey said. It just takes one employee to expose your organization to risk. He recommends partnering with organizations such as the Multi-State Information Sharing and Analysis Center.

- Balance customer service with security: "People tend to jump into their customer service role to help their customers when people should be questioning suspicious activity more often," Condrey said. Risk planning and profiling is just as important as great customer service. "The more lines of business you have, the more complexity you'll have in your organization." He recommends ensuring that risk profile is brought to an acceptable level before developing a larger customer service profile.

ALIGNING CYBERSECURITY TO AGENCY MISSIONS

An interview with Scott Montgomery, Vice President & Chief Technical Strategist at Intel Security

What's the point of cybersecurity? If you ask a security professional, she will likely say the goal is to prevent network intrusions and halt cyberattacks when they occur. But if you ask Scott Montgomery of Intel Security, a security solutions provider, you will get a very different answer.

"It's not about information security for information security's sake," he said. Instead, cybersecurity's purpose is to help an agency achieve its ultimate mission of serving citizens.

To illustrate what he was talking about, Montgomery related an unexpected conversation he had a with a Defense Department leader, after finding significant malware on their network. He was explaining the issue in technical terms to no avail. The agency leader wasn't sure what action to take or why he should take it, even though Montgomery was explaining the technical fallout from the malware.

"[The agency head] said, 'All I want from the network is for me to be able to fulfill my mission. I don't care about the information security and privacy, specifically. I just want to be able to fulfill my mission,'" recalled Montgomery.

This conversation led Montgomery to re-evaluate the way he framed the topic of cybersecurity. "What I realized was, as information security practitioners, we're not exposing non-technical leadership to the problem in language that they understand," he said. "Security practitioners have to start changing that language."

This new conversation is what Montgomery calls an outcomes-based approach to security. Rather than focusing on technical solutions to technical problems, he advocates framing security concerns within the broader picture of mission attainment.

In that same conversation with the DoD leader, Montgomery asked, "Do you use this network and the data on this network to make decisions to support your mission? What if the adversary altered that data? Will that allow you to fulfill your mission cleanly?"

Asking those outcomes-focused questions got the agency leader's attention and also helped inform how they should respond to the network vulnerabilities. Montgomery said this approach should be applied to every cybersecurity decision, from technology to training.

When deploying cybersecurity tools, consider how the management of those tools will impact your IT professional's ability to support the agency mission. "If we have the same administrator responsible for a variety of different activities, then making those activities as efficient as possible is the first, best task that the organization can fulfill," said Montgomery.

One way to achieve that goal is to provide an integrated security solution, because managing multiple solutions in disparate settings requires more time and training. "Say you have eight different vendors on a given server. In order to be effective, that means you're spending eight times the [routine] amount of training," said Montgomery. "If each training class is for a week, you are spending two months of the year away from the console – away from mission – training for those disparate functions. And then you're spending some portion of your workday looking at each one of those consoles."

"It's just bad math," Montgomery continued "These same employees have non-security tasks – mission enablement tasks – that they have to fulfill. That's where they should be spending their time."

Instead, cybersecurity strategies should focus on consolidating and simplifying IT management tasks so that more time can be spent on effectively pursuing mission goals. That's what Intel's integrated security suite supports. "Our responsibility is to make operations and analysis as painless as possible and as least time consuming as possible," Montgomery said.

At the same time, Montgomery said security solutions should create an IT architecture that fully supports the mission's information goals. He mentioned the Internet of Things (IoT) as one mission-enhancing capability that must be accommodated by cybersecurity tools.

"Everybody's first step with respect to IoT is to say, 'We're going to segment it away and have it all on its own network,'" he said. "But people are going to find you can't do that because you actually want the data that comes back from those gadgets in the production network." Instead, Intel creates solutions that can protect that data, as well as other confidential data, within the same network and technology suite.

This integrated approach that focuses on capabilities and outcomes is exactly what's needed to ensure that security efforts don't derail government missions. Integrated solutions ensure that IT professionals manage fewer consoles, require less training, and have a better view of the organization's cyber infrastructure. Ultimately, it leads to better cybersecurity, which in turn leads to a better agency able to fulfill its mission.

CROSS SECTOR SECURITY

Hackers target every sector and often use the same tactics, tools, and techniques across environments. That means that each industry and level of government has a lot that it can learn from colleagues in other sectors. Yet traditional sector silos impede information sharing and coordinated action. Creating holistic cybersecurity will require a reconsideration of privacy laws, organizational structures, and communication pathways between and across sector verticals.

10

11

12

Trend #10:

INFORMATION SHARING PATHWAYS

Forming a process and team to coordinate disparate sectors and facilitate the sharing of cyberthreat and patching information

WHY IS IT IMPORTANT?

For private companies, cybersecurity information sharing is difficult. Even as they work internally to classify and address threats, companies should provide relevant information of that threat to other organizations. That requires navigating government bureaucracies to alert the appropriate agencies and people, and identifying industry partners who might be affected.

For government organizations, the task is no less complex. Once they receive or discover threat information, relevant security agencies must make sure news of it is dispersed to all stakeholders, including those it has not yet impacted. If the vulnerability could affect a government system, it must be repaired immediately.

To make matters even more challenging, all of this has to happen in near real time if cyberthreats are going to be prevented from becoming true breaches across sectors and organizations. In these situations, coordination is paramount to quickly collecting and disseminating information.

That's why President Barack Obama signed an executive order on Feb. 13, 2015, "Promoting Private Sector Cybersecurity Information Sharing." It calls for cross-sector organizations to collaboratively create information-sharing and analysis organizations (ISAOs) that institutionalize the procedures, formats, and expectations of cyberthreat data sharing.

WHO IS DOING IT?

Gov. Chris Christie authorized one of the first state-based ISAOs in May 2015. Less than three months since its launch, the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) is already fulfilling its mission to defend the state's "digital density" by acting as a "one-stop shop for cybersecurity information sharing, threat analysis, and incident reporting." NJCCIC executes three primary tasks: coordination, assessment, and education.

The cell connects state public organizations, including the New Jersey State Police, Office of Homeland Security and Preparedness (OHSP), and Office of IT, with industry members. NJCCIC acts as a hub for information sharing by allowing any entity to report incidents or threats, and it coordinates responses across government and non-government entities in the event of an attack. The organization also maintains relationships with several federal partners including DHS, the Justice Department, and the Secret Service to better contextualize and counter widespread cyberthreats.

With that information collected across sectors and levels of government, NJCCIC can then produce holistic threat analyses for the state. On request, the cell will also produce sector-specific threat analyses for its members. These assessments cover the "the entire attack lifecycle, from the technical signature to the motivations, affiliations, and tactics of the actors." When vulnerabilities are detected, NJCCIC informs stakeholders of the issue and offers risk-based suggestions to buffer security.

Finally, NJCCIC also provides educational materials to government personnel and the community at large. Evergreen resources educate users on common cybersecurity tactics. NJCCIC provides a series of publicly accessible cybersecurity tips for Internet users and links to the Center for Internet Security's Cyber Hygiene Toolkits. Timelier information, including private sector cyber incident announcements and vulnerability discoveries, is provided in real time on the cell's website and Twitter feed.

Ultimately, NJCCIC is meant to provide a common cyber context for all New Jersey stakeholders because, as OHSP notes, "Shared situational awareness drastically mitigates the attacker's offensive advantage by enabling the observation of one to bolster the defenses of many."

Trend #11:

MULTILEVEL GOVERNMENT COLLABORATION

Pooling cybersecurity funding, technology, intelligence, and/or personnel from local, state, and federal governments to reap the benefits of shared resources

WHY IS IT IMPORTANT?

Each level of government has its own perspective on cybersecurity and threats. For instance, local cyber authorities — most often public-safety and law enforcement officials — maintain a detailed view of local trends and populations. Even cyberthreats can have physical domains, after all.

State authorities can monitor more widespread threats while still maintaining a tight coordination capability and focus, given the defined scope of their domain. Finally, federal agencies keep an eye on agency-specific threats and nationwide concerns that are often more sophisticated and far-reaching than localities could address.

Yet although each level of government maintains its own cyber capabilities, its ability to safeguard networks and infrastructure exponentially increases when the levels pool resources and networks. Together, state and local governments are able to bolster their response efforts with more manpower and better technology. They can also deploy better countermeasures informed by national context and intelligence.

Even federal agencies, which often have the biggest budgets and largest fleet of cybersecurity personnel, can only do so much alone. Consider how difficult it would be for the FBI to pursue a U.S.-based hacker group without eyes on the ground, intelligence about local crime, and a standardized network that investigators could navigate.

To reap the most return on cybersecurity investments, every level of government must pursue partnerships to share resources.

WHO IS DOING IT?

In July 2013, the Utah Department of Public Safety (UDPS) partnered with its regional FBI field office and the FBI Internet Crime Complaint Center (IC3) to establish a pilot program called Operation Wellspring for sharing information and coordinating investigations into cyber fraud across the state and federal government. The partnership allows the appropriate levels of government to tackle cyber incidents, while also enabling organizations to pool investigative resources.

By granting other agencies access to the more than 3 million complaints in the IC3 database, the FBI empowers Utah officials to take over cases within their jurisdiction. "Because not all Internet fraud schemes rise to the level necessary to prosecute them in federal court, we are enhancing how we package the investigative leads we receive at IC3 and disseminating those packages directly to state and local agencies," explained Richard McFeely, Executive Assistant Director of the FBI's Criminal, Cyber, Response, and Services Branch. This sharing alleviates the burden on taxed FBI resources and personnel who would otherwise have to pursue these low-level cases.

Conversely, if a cybercrime is detected in Utah that originated elsewhere or affects citizens across state lines, the state cyberunit can leverage the FBI's investigative resources to trace the threat across borders. For instance, in one case, Utah officials traced an attack to South Africa with FBI assistance.

In either scenario, "all cases are worked in a coordinated manner, with knowledge and expertise shared across all investigative and analytic activities," UDPS Keith Squires Commissioner said.

Today, the program has moved from the pilot stage to become fully operational. Following a number of initial successes in Utah, FBI field offices in Dallas and San Diego are also seeking to establish this partnership model.

Trend #12:

THE COMPETITION FOR IDEAS

Creating competitions to surface and fund innovative processes, tools, and technologies for cybersecurity from the public or private sector

WHY IS IT IMPORTANT?

If you have any exposure to government, you know that procurement is a pain point for every agency and project. Nowhere is this as true as it is in the field of cybersecurity because traditional processes of technology development and acquisition directly contrast the way cyberthreats are executed.

Hacks occur in real time, but procuring technology to counter that attack can take months or even years. Cyberthreats constantly evolve, but technology requirements are often defined upfront and then remain static throughout the product development cycle. And private sector organizations have greater exposure to hacks and therefore more real-world insight into what makes the best solution, but traditional acquisition procedures mandate that government bodies define what cybersecurity technology should look like.

Simply put, traditional procurement routes make it nearly impossible for government to effectively collaborate with industry to create timely solutions to today's cyberthreats. As a result, many agencies seek ways to circumvent or alter that process to get better solutions faster.

One such method is the challenge, in which agencies don't define a solution to be acquired. Instead, they present a problem and ask private sector experts to solve it. This method of acquisition can often be quicker and cheaper than traditional procurement routes and it produces better, more collaborative products.

WHO IS DOING IT?

Challenges vary in complexity and scale, depending on the needs and resources of the funding agency. Unsurprisingly, one of the largest challenges on the federal scene comes from its largest agency: DoD. Launched in 2014, DARPA's Cyber Grand Challenge (CGC) is a multiyear effort to create an automated security system that can identify and patch vulnerabilities in real time, before a breach can occur.

Although DARPA is known for its in-house, high-dollar technology projects, CGC is an example of the agency's increased effort to bring in industry ideas. The challenge is organized as a tournament, with each round testing participants in a "Capture the Flag" contest. In the simulations, non-DoD experts deploy custom-built computer systems that reverse-engineer software to identify its vulnerabilities and replace them with secure patches.

These systems are tested within DARPA's Experimental Cyber Research Evaluation Environment, which is open sourced to ensure constant evolution, similar to what we witness in real-world information systems. It also adds another level of public collaboration to the government exercise.

Of the 104 teams who entered the contest, seven remain. The finalists include members of both industry and academia, and they get a year and $750,000 to prepare for the final competition, to be held in August 2016. There, DoD officials hope to find the ultimate automated security system.

The CGC winner will be awarded $2 million, while the runner-up will receive $1 million and third place will get $750,000. That's a small price to pay for the "automation revolution" that DARPA officials hope to create through this challenge, said Program Manager Mike Walker. What's more, the total cost of the competition will still pale in comparison to what it would have taken to build and test a similar program internally.

Information Sharing

The case studies in this section highlight how agencies are partnering with one another and the private sector to build cross-sector security. However, many argue that a governmentwide effort to re-imagine privacy and sharing laws is required if true cybersecurity partnerships are going to succeed.

Currently, many private companies are hesitant to disclose breach information to government organizations out of fear of enforcement action against them related to revealed faults in how they prepared or responded to the attack. In a classic catch-22, companies may be held liable for mishandling an event by seeking assistance to better handle it. But when that information is withheld, the government loses critical intelligence on how hackers are targeting industry.

Many lawmakers agree that although individual agreements and partnerships can facilitate information sharing on a small scale, national legislation will ultimately be necessary to provide companies with the liability protections they desire. Beyond that, companies and privacy advocates want to ensure that government is using their shared information solely for cybersecurity, rather than surveillance.

Currently, Congress is considering three bills that would address the public sector's concerns: the Cybersecurity Information Sharing Act (CISA), National Cybersecurity Protection Advancement Act, and Protecting Cyber Networks Act.

With the exception of cases of gross negligence or willful misconduct, the first two would shield companies from civil or criminal enforcement that is the direct result of information sharing. The third offers slightly fewer protections because it limits only liability related to information sharing done in good faith.

All three offer some level of guarantee regarding the use of personally identifiable customer information once it's handed over to authorities, though CISA is argued to be the most vague in its protections.

2015

FIREEYE CYBER DEFENSE SUMMIT

MIRcon

OCTOBER 12 - 14, 2015 | WASHINGTON HILTON | WASHINGTON, DC

KEYNOTE SPEAKERS

DAVE DEWALT

GENERAL COLIN L. POWELL, USA (RET.)

KEVIN MANDIA

EVENT HIGHLIGHTS

NETWORKING

Share Expertise
Talk best practices
Build Relationships

PROFESSIONAL DEVELOPMENT

Learn from industry peers
Find out about cutting edge tools
Learn network management
Earn CPE Credits

3 TRACK SESSIONS

Learn IR best practices
Dive deep on Malware
See what's next in cyber security
Hear about customer and partner case studies

TECHNOLOGY IN ACTION

Hear real-world applications
Watch tech in action
Leverage peers to problem-solve
Learn from FireEye partners

PRE-SUMMIT TRAINING

Four 2-day course before the Summit
Malware Analysis Crash Course
Enterprice Incident Response
Eterprise Incident Response with MIR
Endpoint Security Deployment and Administration

CODE OF ARMS RECEPTION

Celebrate in style
Join us - and fellow attendees - for drinks, food, music and games

KEY DATES

SUNDAY
OCT 11
TRAINING DAY 1

MONDAY
OCT 12
TRAINING DAY 2
WELCOME RECEPTION

TUESDAY
OCT 13
SUMMIT DAY 1
CODE OF ARMS RECEPTOIN

WEDNESDAY
OCT 14
SUMMIT DAY 2
GOVERNMENT BREAKFAST

Register today *(free for Government employees)* at **www.fireeye.com/summit2015**

CYBERATTACKS KNOW NO BOUNDARIES

An interview with Tony Cole, Vice President and Global Government Chief Technology Officer at FireEye

Unlike the physical world around us, there is no distance in cyberspace. That's great for collaborating with employees around the world or for accessing files when working remotely. But the same Internet-based services we use to increase productivity are also targets for hackers and nation states to exploit, said Tony Cole of FireEye, a cybersecurity company.

"Back in the '90s, there really weren't a lot of resources focused on solving this problem, simply because there wasn't much awareness of the growing importance of our interconnected enterprise systems in government," Cole said. "A lot of people didn't realize that there would be ample opportunity for organized crime and other nation states to move their espionage practices online."

Today, there are well over 55 nations armed to conduct espionage in the cyber realm, Cole said. Those nations are far more sophisticated than they were two decades ago, and governments are still challenged with defending themselves and their data in cyberspace.

That's why FireEye is working closely with governments at all levels to help them detect, prevent and respond to advanced cyberattacks. The security firm specializes in:

- Continuous monitoring capabilities that allow agencies to automatically detect ongoing attacks
- The use of global threat intelligence to profile potential attackers
- Capabilities to quickly prevent or contain attacks using detonation chamber technology as recommended by NIST

Still, there's more work to be done.

"Governments have a long way to go to put the right policies and architectures in place, so that they can actually minimize the impact," Cole explained.

Education and awareness for employees is critical since organizations can't afford to take awareness training lightly, and they can't assume an annual online course is enough to educate their workforce. Cole noted one Silicon Valley firm that uses gamification to drive security awareness company-wide. When employees alert the security department of spear phishing emails or report other cyber and physical security vulnerabilities, they get points that can then be used to buy things.

For government agencies, gamification may be a cost-prohibitive means to boost security awareness, but Cole encouraged agencies to consider methods that make training an on-going process that keeps security at the forefront of all employees' minds.

That's a must, because all it takes is one person clicking on a link, a weaponized attachment in a malicious email, or one exploited security vulnerability in the supply chain to give hackers an advantage. No government agency is immune to cyberattacks, and it's virtually impossible to stop every attack. If a system is breached, agencies must be prepared to detect the breach quickly and minimize the impact.

But that is easier said than done, considering it takes an average of 205 days from the time an attacker breaches a system to the time an organization detects it, Cole said. That 205-day period is known as dwell time.

And, most often, organizations don't detect the breach on their own. Instead, a law enforcement agency, a computer emergency response team, or another outside organization notifies them.

Cole's advice to agencies: Hunt in your environment to determine if you've been compromised and don't rely on just signature based defenses.

Good hunters know the difference between normal activity and anomalous activity on their network. If all of a sudden users log onto the network from Romania, that should raise a red flag. Did someone move? Is there a new remote employee? Or has the system been compromised?

"Agencies need to look for anomalous activity in their networks and external communications, as well as forensic artifacts that can be found inside their network, too," Cole said.

FireEye partners with agencies to conduct compromise risk assessments and help them with their hunting, Cole explained. "We go in and hunt in their environment to show them indicators of a compromise," he said. If the agency has been compromised, FireEye shows agencies how to lock down their systems and recover.

Cole said until recently, many organizations still don't see themselves as targets for cyberattacks. But massive breaches like the one directed at OPM have forced everyone to consider how their data — if compromised — could create a full picture for hackers looking to harm them or their allies.

State actors target contractors, subcontractors, partner agencies and seemingly obscure third-party organizations that do business with the government to ultimately gain access to sensitive government assets.

"We're all in this together," Cole said about cybersecurity and its global impact. "We've got a lot of allies around the globe, and many of those attacks can go through them to get to us, or vice versa. We need to talk more about information sharing and best practices from a global perspective."

Interview

AN UPDATE ON THE NIST CYBERSECURITY FRAMEWORK

An interview with Matthew Barrett, a Program Manager of the Computer Security Division at NIST

Matthew Barrett, a Program Manager of the Computer Security Division at the National Institute of Standards and Technology, answered our questions about how the Cybersecurity Framework is being leveraged to improve the security of critical infrastructure, and what's next for the project

How do you determine who is using the Framework, and in what ways?

Sometimes organizations ask us for information about using the Framework, so we have visibility into their emerging implementation. We also note media reports, conference papers, and presentations that highlight Framework use. As balanced against other activities, we reach out to those organizations to offer guidance, and so we can get first hand knowledge of what real application and adaptation of the Framework looks like. Some organizations, like Intel, publish white papers and have presented on their Framework pilots and implementations.

The cyberframework@nist.gov inbox [for feedback] is there, but we know if we really want a good information share, we have to reach out, have a conversation, and meet people in person to talk.

How do you incorporate implementer feedback into the Framework?

When it comes to Framework evolution, we are running a change control process in the background. So, as we interact with the folks and they say, "Well this part of framework is particularly valuable, love it," we take note. Also, as they say, "Well, we would love to see this change or that edit," we take note.

Those comments feed a change control log, which is a summation of those industry interactions, what's coming to the inbox, and public case studies. The change control log will provide our initial direction when it's time for an update.

When we were developing Framework, what we often did is we took comments through the feedback inbox and we sent out requests for information. Then, we tried to identify trends where we were hearing more than one voice on a given topic. We would take those trends to a place where we could have a larger discussion, like a workshop. That discussion kind of looks like this: "Here's the trend NIST heard. Did we hear you right?"

What have you learned from your conversations with implementers?

"We want to make the connection points between the various bodies of NIST work - for instance, information sharing, privacy, cybersecurity education... basically all of the Framework Roadmap items - more apparent to agencies and industry."

Matthew Barrett
Program Manager, Computer Security Division,
National Institute of Standards and Technology

Within industry, one adaptation people are making is to augment the Implementation Tiers concept. People like the concept, but they are adding to it, which is great. It makes me wonder if we might expand on that concept just a little bit in future versions [of the Framework]. Another critique we have heard is that folks would like to see cyberthreat intelligence work better represented in the Framework.

On the federal side, there's a question how agencies might use the voluntary Framework alongside their important and mandatory FISMA practices. We hear, "How can I use those things together to get a greater value?" That voice is becoming louder and louder, and it needs to be answered. We have the full intention of answering it.

How are you addressing these concerns from industry and government?

Another thing that you will see in any update that's coming is a more clear delineation of where the system security engineering fits in the world of the Cybersecurity Framework. To accomplish this, I am collaborating with Dr. Ron Ross on where Framework intersects with the systems security engineering practices in Special Publication 800-160.

We want to make the connection points between the various bodies of NIST work - for instance, information sharing, privacy, cybersecurity education... basically all of the Framework Roadmap items - more apparent to agencies and industry.

Until the next version of the Framework is published, how are you updating the public on implementation?

We just published a newsletter that is not only an update about what NIST has been doing, but also an update on some of the things that we've observed in industry. This newsletter certainly has some of the noteworthy observations from our side.

Other ways to get the pulse is to check the website itself where we have the latest frequently asked questions. At the website we also publish industry resources, which are publicly available and free resources. As NIST speakers commit to events, we also list those events at the website. It is more of a living site nowadays.

When will we see a new version of the Framework?

The update timeline is not set. Industry will let us know if there's a critical need. As prompted by industry, NIST convenes activities to update Framework. At that time, we will likely use a combination of RFIs and workshops to gather input. Then ultimately we will release online documents in draft as we have in the past, for industry to continue commenting.

What are your top priorities in the near-term?

There are still some communities and sectors that we want to reach a little bit better. For instance, the small and medium business community – it's such a large demographic that we want to make sure we give it proper treatment.

And it's also interesting for other reasons, too. It's not unusual for a small organization to have a large number of assets that are not in their direct management. For instance, you go to a service provider for email, document management, calendaring, etc. So, that's the community that we want to make sure that we reach strongly.

We also want to answer that "getting started" question and get the word out there. We are actually working on some online learning materials to supplement our public speaking.

Identify and Defend Against Cyber Threats with Big Data Analytics

ViON Cyber Secure Provides Big Data Cybersecurity on a Pre-Configured, Fully Integrated Platform

- Read the White Paper
  Big Data and Analytics: **Effective Tools to Enhance Security**
- See the top 5 issues facing CSOs. Download the
  Cyber Security Infographic
- Learn more about **DataAdapt Cyber Secure**

cisco Gold Partner

ViON

NetApp

196 Van Buren Street | Herndon, Virginia 20170 | (571) 353-6000 | (800) 761-9691 | vion.com

AUTOMATING SECURITY TO CREATE VIRTUAL TRUST

An interview with Richard Breakiron, Senior Director of Cyber Solutions at ViON

"Security is all about trust," said Richard Breakiron of ViON, an information technology enterprise solutions provider. But how do you create that trust in the realm of cybersecurity, where users are remote and their identities are more difficult to verify?

Breakiron said the first impediment to a more secure cyberspace is a lack of critical attention to the risks of unsafe behavior. "What happened at Anthem, Target, Home Depot, and J.P. Morgan - those numbers are in the millions," he said. "If those had been physical casualties that walked into emergency rooms in the United States, the reaction of the American citizenry would be very different. But because it's virtual, people don't have an appreciation for the dramatic problems that have occurred due to the missteps of just one or two employees."

However, as the fallout from these attacks is increasingly felt by corporations and governments, Breakiron said we can expect to see more focus on cybersecurity best practices and identifying users who fail to uphold the practices.

Actually, Breakiron said cybersecurity isn't that different from real-world security. For instance, he related it to security on the highway. As you drive, you trust that other drivers are licensed, following traffic rules, and maintaining safety to the best of their ability. However, that's not always true and, in those cases, the security of everyone is compromised.

Similarly, network security can be compromised if a single user is breaking the trust of their colleagues and using bad cyber practices. "If there's a weak link in physical trust and I lose my keys, my house is vulnerable. When I lose the virtual key, the entire network is potentially vulnerable," said Breakiron.

So how do you strengthen that weak link? Breakiron said the key is to establish a virtual trust with your users. That process comprises four basic steps:

- Identity Management - Creating a virtual profile for an individual
- Authentication - Verifying that the user's password, actions, and device match the established virtual profile
- Access Control – Granting access privileges to certain data and systems based on rules tied to that virtual identity
- Verification and Analytics – Auditing and tracing the first three steps

As cyber professionals implement this process, however, Breakiron emphasized a need to make sure they keep the end user in mind. "I want to maintain freedom of movement in the cyber domain," he said. "I want to be able to log onto the network and share a credit card freely, knowing I can buy something, knowing that I'm not at risk doing that, because I love that convenience. But we have to come up with weighs and balances of the risks, relative to the rewards and the gains that we get from this capability."

To efficiently execute this process and quickly establish virtual trust with end users, Breakiron said we are going to see cybersecurity strategies take a "Google car approach". In the same way that self-driving cars mitigate the risk of bad drivers endangering our roads, automated security solutions will decrease bad cyber habits. "Our trust at the individual level is going to be automated. We recognize that [some users] don't follow the rules… so we're going to automate the rules," Breakiron said.

In other words, when a link in this virtual trust chain is broken, solutions will create automated alerts and even take automatic actions to prevent a user from damaging a network. This automation will largely depend on the ability of these solutions to process massive amounts of data quickly, analyzing it for indicators of bad behavior and creating alerts when they are discovered.

"Once you understand how the mechanics of individuals and how business processes work, you try and devise ways to automate it. You come up with algorithms on how you can interpret data and make decisions," Breakiron said. "What you see in industry today - what ViON and YaData are doing - is they're bringing automated, next generation capabilities that rely on much faster computer processors, much faster software, and much more intelligent software to automate security."

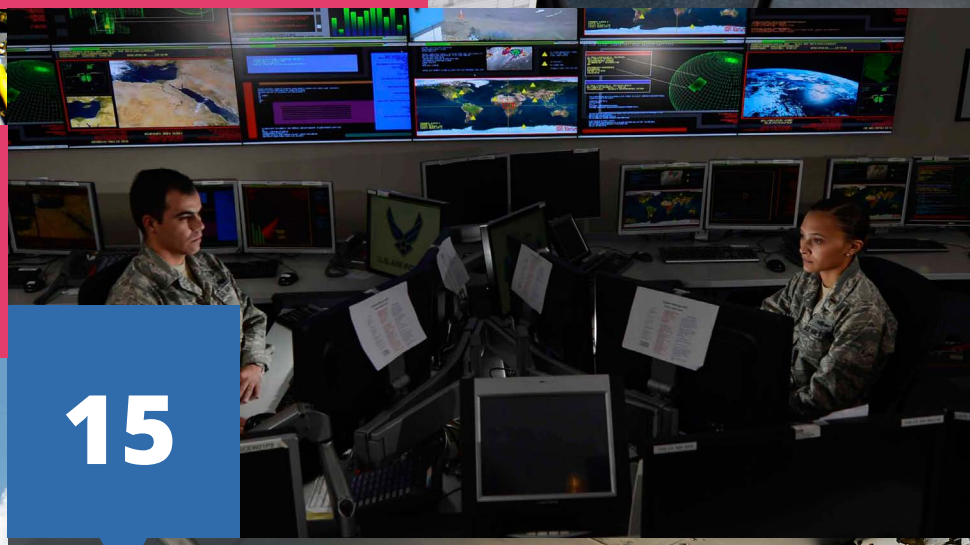
Breakiron said security is about trust. Yet it is also about having a plan when that trust is broken. With this ability to analyze large amounts of user data at rapid speeds, cybersecurity professionals can assuredly create virtual trust with their ends users. When that trust is broken, that weak link can be quickly identified and corrected.

SECURE BY DESIGN

Most government IT architectures were built without cybersecurity as a primary consideration. Now, those legacy systems present grave risks to security as cyberthreats mount. While some organizations attempt to tack security tools onto existing systems, most agency officials realize they need a new approach. Security by design, in which strategies and tools are ingrained with security before deployment, is the only way to ensure that we are prepared for the cyberthreats of today and tomorrow.

13

14



15

Trend #13:

CONTRACTING FOR SECURITY

Ingraining security in the requirements and design of technology, rather than supplementing tools with security add-ons after it is deployed

WHY IS IT IMPORTANT?

Government processes are slow. The technology is old and there's no budget to replace it. Government doesn't have enough staff to really become secure. It may simply never have the security that private companies have.

In the past, these idioms have defined the way many professionals see government IT and cybersecurity. And although these may be true in many scenarios, they are no longer viable reasons to accept information insecurity. As it becomes increasingly obvious how much is at stake in our information systems, government IT shops must overcome these obstacles of slow procurement, legacy systems, and staff shortages to create more secure IT architectures. Then, they must make sure they don't run into these challenges again.

One way to do so is by requiring that security be built into every technology acquired, rather than just cyber tools. By including cybersecurity considerations in an original acquisition, agencies avoid having to buy separate technologies to tack on security later. Additionally, they can automate capabilities into their tools at the onset, rather than relying on cybersecurity personnel to create monitoring solutions after technology is deployed. At the same time, IT professionals can have greater confidence that their security systems will be effective because they will be integrated with non-security tools by design.

WHO IS DOING IT?

The Federal Risk and Authorization Management Program and other federal programs are working to ingrain security by design in federal technologies. However, many federal bodies are also creating standards that can be applied to local and state government technology acquisition processes, even as the procedures themselves differ.

For instance, the FBI created a series of guidelines, called the Criminal Justice Information Services (CJIS) Security Policy, for cloud service providers. "Criminal justice information needs good security because it is information about citizens, often at their most distressed and vulnerable," said former DHS Secretary Michael Chertoff. "Fortunately, law enforcement agencies have a good model to consider adopting when storing data in the cloud, one that addresses both security and privacy issues."

The International Association of Chiefs of Police (IACP) recommended that the policy be applied for all criminal justice systems in law enforcement. Now, local departments including the Los Angeles Police Department (LAPD), the San Bernardino County, Calif., Sheriff's Department, and the Oakland, Calif., Police Department are starting to use those standards in their cloud purchasing processes, rather than attempting to apply security standards to legacy systems.

"In an ever-increasing threat environment, where the Internet and systems are continually being targeted, we decided that all our systems should meet CJIS requirements across the enterprise," said Ted L. Byerly, Team Leader for Networking, Security and Infrastructure at the sheriff's department.

Byerly's department, like LAPD and Oakland PD, chose Microsoft's Azure Government platform, after committing to building cloud environments that met CJIS requirements. What's more, each contract ensured that these requirements would continue to be upheld even as the IT architecture and risk environment of each law enforcement team changed.

Trend #14:

RISK-BASED SECURITY

Targeting and eliminating vulnerabilities to known or unknown cyberthreats, rather than countering them as they manifest

WHY IS IT IMPORTANT?

Today, breaches are inevitable. But that doesn't mean agencies should wait around for them to happen. Fighting cyberthreats follows the same logic as any other battle: If you practice only defense, your opponent will always have the upper hand. And when you lose your fight and suffer a breach, you'll be worse off because you won't be prepared to counter that unique attack.

Instead of waiting for the breach, agencies must proactively assess their networks for vulnerabilities. This risk-based approach, which is heavily advocated by NIST's Cybersecurity Framework, provides three primary benefits to any cybersecurity organization.

First and most obviously, acting on your vulnerabilities reduces hackers' attack vectors, thereby diminishing your likelihood of being breached. Second, a risk assessment gives you a better idea of where you are more likely to experience an attack, so even if you can't prevent it, you can prepare to counter it when it occurs.

Finally, risk-based assessments provide common value across agencies and industries. A weakness in your organization is very likely duplicated in other agencies given the many common operating procedures and tools of government organizations. Therefore, one agency's risk-based assessment can result in improved cybersecurity for all.

WHO IS DOING IT?

The Virginia Information Technologies Agency (VITA) was ahead of the curve when officials there decided to survey the state's IT enterprise for vulnerabilities in January 2013. From that survey, they identified two key cybersecurity risks — unnecessary administrative rights and Java.

Following those discoveries, VITA implemented a 90-day project to provide IT and security services for 89 executive branch agencies. The project was focused on updating agency applications to re-provision local administrative rights solely to staff who needed elevated access privileges to conduct their business. The project also analyzed Java levels for each agency and identified deficiencies.

In addition to VITA staff, the Commonwealth Information Security Council and CIO Council collaborated on the project to provide insights about Virginia's current infrastructure. Benefits of the project included a reduced likelihood of successful cyberattacks affecting employee workstations, business processes, and websites.

Malware incidents were reportedly reduced to the lowest level recorded. Additionally, there was a 54 percent reduction in security incidents, which saved about $450,000 between August and December 2013. Each security incident is estimated to cost about $600.

The number of accounts with unnecessary administrative rights was reduced from 73,519 to 10,922, or by 85 percent. Approximately 35,000 instances of Java on employee computers were updated to appropriate security levels. State government, federal entities, business leaders, and citizens alike can now benefit from using Virginia state agency websites and applications to conduct their business, knowing their information is more secure than before.

Trend #15:

ADAPTIVE TECHNOLOGY

Leveraging technology that autonomously adapts to new threats and environments

WHY IS IT IMPORTANT?

We have said it numerous times in this and other research guides, but it bears repeating: Cyberthreats constantly evolve. And because that is true, government's approach to cybersecurity must also continually change. Yet even if government speeds up procurement to get new technologies faster and changes tactics to use those technologies in a risk-conscious manner, hackers may still be able to get ahead if the technology itself remains static.

The only thing differentiating a hazardous legacy system and a secure new one is time. But that doesn't have to be the case. If technologies are ingrained with the same agility that hackers have, cyber systems can endure attacks, learn from them, and become more prepared for the next ones.

This fact isn't lost on government. In fact, the most recent "Trustworthy Cyberspace: Strategic Plan for the Federal Security Research and Development Program," created by a working group of federal agencies, included a "Moving Target" research theme. That mandate called on agencies to, "develop, evaluate, and deploy diverse mechanisms and strategies that dynamically shift and change over time in order to increase complexity and costs for attackers, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency." Now, many agencies are accepting that challenge.

WHO IS DOING IT?

The Air Force Research Laboratory (AFRL) is taking a multipronged approach to creating a comprehensive suite of adaptive technologies for cybersecurity. This attempt began in 2011 with the establishment of the Cyber Agility Initiative.

Under the auspices of that initiative, the Polymorphic Machines and Enclaves Program was launched a year later to "create rapidly shifting network architectures with automated agility and diversity mechanisms to modify or morph the network continually, dynamically, and unpredictably into secure operational modes, both before and during attacks." In other words, the computers' and networks' characteristics change in a pattern that is seemingly random to attackers, making them more difficult to target.

Around the same time, AFRL created an Active Repositioning in Cyberspace for Synchronized Evasion technology that constantly changes the network identity of hosts — a process called Internet Protocol address hopping — to confuse and evade hackers. That program is now entering pilot stages at other agencies.

Like the technologies it hopes to ingrain in government cybersecurity, AFRL is adapting the way it seeks solutions to this problem. Now, AFRL hopes to expand its cadre of technologies through the procurement of industry solutions that promote cyber resiliency. Adaptive technologies continue to be a major focus in this new initiative to "modify the cyber domain in favor of mission assurance."

The 2014 Broad Agency Announcement identified four "thrust areas" to create greater resilience. Two focused on adaptive technology:

1. Self-protecting software systems: Systems that use domain knowledge and mission needs to defend against malicious attacks or failures and can anticipate and mitigate future security threats.

2. Machine-generated repair: Automatically generate repairs to code and corrupted data to recover with immunity.

From providing a soldier secure access to mission-critical data in the field to providing citizens services across the web, the federal government demands the most innovative and scalable IT solutions available. Symantec information management and security solutions help government agencies empower their employees to achieve their goals. When you can do it simply, safely, and quickly, you can do it all. Start doing more at go.symantec.com/federal

#GoEmpower

Go ahead, you've got Symantec™

CYBER TRENDS THAT WILL SECURE PLATFORMS BEFORE THE BREACH

An interview with Ken Durbin, Unified Security Practice Manager at Symantec

In the wake of a several high-profile data breaches, government agencies at every level have been scrambling to shore up cyber defenses. Looking for ways to better defend their data and users, the public sector is turning to cybersecurity experts at companies like Symantec for solutions. GovLoop sat down with Symantec's Ken Durbin to discuss the cybersecurity trends his organization is seeing in the public sector and the tools government agencies can use to modernize their cybersecurity platforms.

According to Durbin, government agencies must defend against both external and internal threats to adequately protect their data.

ADDRESSING THE EXTERNAL THREAT

To help minimize the external threat, government agencies are looking to enforce two-factor authentication and meet the standards set by the DHS's Continuous Diagnostics and Mitigation (CDM) program. Durbin explained, "CDM was designed to make sure that federal executive branch agencies all have a common level of cyber protection."

Before CDM, the level of cyber maturity varied greatly between agencies. "Some people had a really good handle on where all their assets were located, while other people did not," Durbin said. To level the security playing field, the federal government had to go back to the basics. CDM's first phase, which involves locating hardware and software assets, verifying configurations and identifying known vulnerabilities, is currently underway.

"A lot of successful attacks today are launched against vulnerabilities that we've known about for years," Durbin explained. Applying the simple steps in CDM's first phase would significantly reduce the number of successful cyber attacks against the government. "Symantec has solutions that will help an agency identify all of their assets, and scan them to make sure they're configured properly and deploy patches, if needed," he said.

Another big cyber trend for government? As Durbin shared, "Identity management and user authentication are getting a lot of attention. People are taking a hard look at who should really have privileges to what, and eliminating privileges that don't make sense. For those people who are supposed to have privileges, they're looking to enforce two-factor authentication to make sure an individual really is who they say they are," Durbin said.

Using Norton Secure Login (NSL), Validation and ID Protection (VIP) and Symantec Identity Access Manager (single-sign on technology), Symantec can help modernize the public sector's user authentication capabilities. "We're on a movement to eliminate the password," he said.

THE HUMAN SIDE OF SECURITY

Government organizations now recognize that malicious and inadvertent insider threats are significant risks to their data. Because they are effective at limiting the severity of a breach, agencies are looking at data loss prevention technologies like Symantec's Data Loss Prevention (DLP) and Data Insight (DI) to mitigate insider threats. These technologies can quickly detect inappropriate access or movement of data, stopping data breaches before they can take their toll.

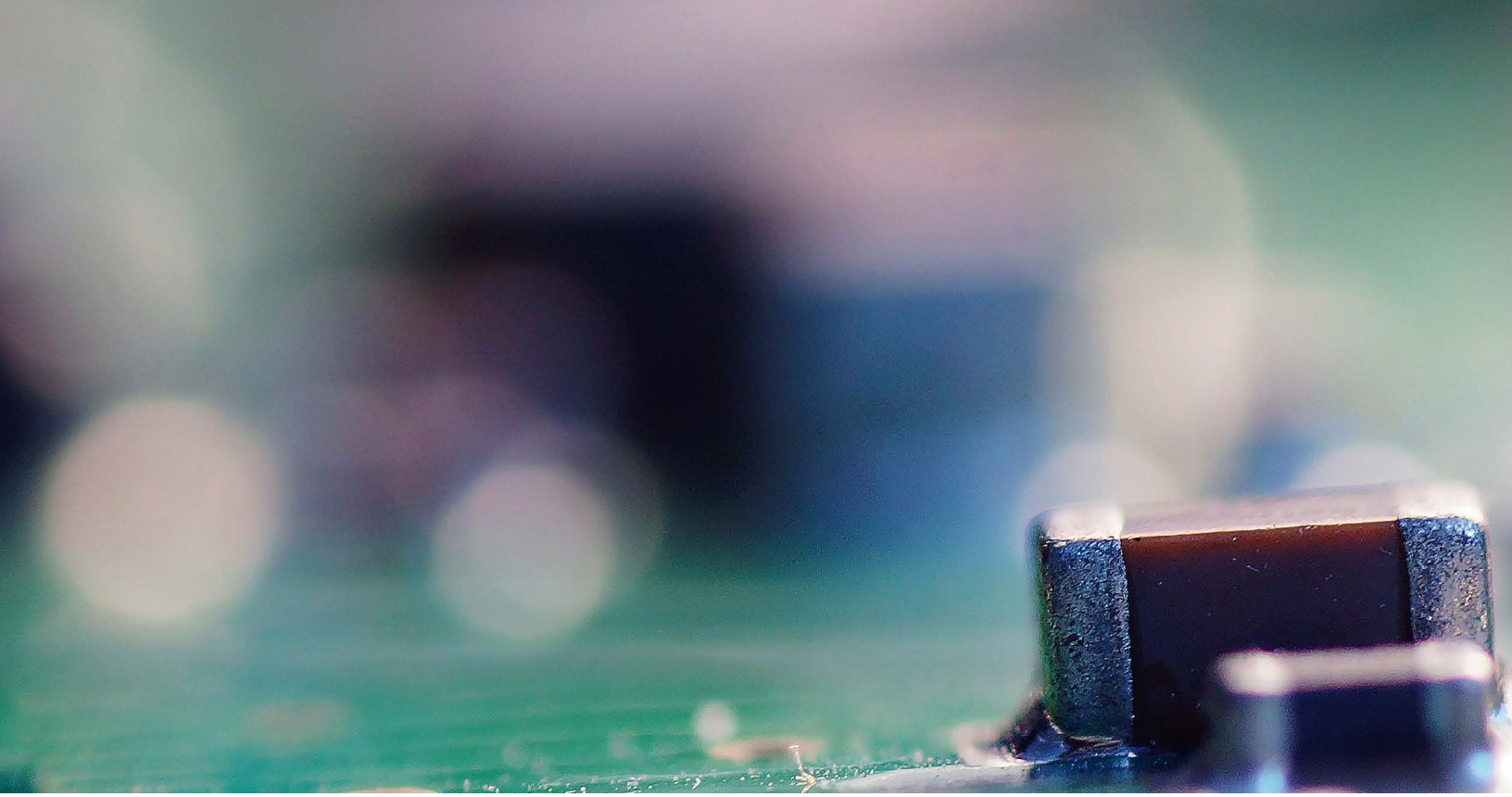
"The next step in the evolution of Cybersecurity is what we refer to as Unified Security. Our Advanced Threat Protection (ATP) solutions will allow our customers to take advantage of Unified Security," Durbin said.

So what is Unified Security? Today, network, endpoint and gateway security tools work independently of each other. "Imagine if those tools were aware of each other and could work together...a network security sensor would detect a threat, and check with the endpoint protection sensor to see if they've seen that threat, and if they did, determine if it had already mitigated it. If the endpoint already mitigated the threat, then there's no need to spend time and resources chasing the threat down" Durbin explained. .

Despite advancing technology, Durbin stressed that effective cybersecurity boils down to preparation. "Unfortunately, we see a lot more interest in our [cybersecurity] solutions post breach...it's almost like locking the barn after the cows have been set free, but it's still essential to prevent another attack," Durbin said. "We're working very hard to have those conversations with our customers pre-breach instead of post."

Symantec also helps government agencies recruit and develop "cyber warriors". Using the safe environment provided by Symantec's Cybersecurity Simulation program, IT applicants and staff can run through attack scenarios, bolster their skills and identify weaknesses, all online, and self-paced.

Symantec is providing government agencies at all levels with the tools they need to secure their data. With modern technology and more qualified personnel, the public sector stands a much greater chance at preventing another major data breach.



Interview

AN UPDATE ON FISMA IMPLEMENTATION

An interview with Ron Ross, a Fellow at NIST

Ron Ross, a Fellow at the National Institute of Standards and Technology, answered our questions about the past, present, and future evolution of the Federal Information Security Management Act (FISMA) Implementation Project.

What does the FISMA Implementation Project do?

NIST was tasked by the Federal Information Security Management Act in 2002 to develop the security standards and guidelines for the federal government that allow federal agencies to protect their information and information systems that support their critical missions and business functions. In 2009, with the formation of the Joint Task Force Transformation Initiative, NIST partnered with the Department of Defense and the Intelligence Community in coordination with the Office of the Director of National Intelligence, to develop a unified set of security guidelines that are used by all federal agencies. In 2014, the original FISMA legislation was updated and renamed the Federal Information Security Modernization Act.

How has the project mission or strategy changed over time?

The core standards and guidelines that we began developing in 2003 have pretty much stayed rock solid over the last decade. They provide the foundation for all of the other guidance documents that we produced including our security and privacy control catalog, our assessment guidelines, and the Risk Management Framework—a complete toolset that helps our customers implement cost-effective, risked-based security programs.

What has changed since 2003 is the threat, and in particular, the pace by which the cyberattacks are occurring. The number of attacks has increased dramatically, as well as the sophistication of those attacks. So, we have transformed our original approach and evolved the standards and guidelines from a static to a more dynamic approach.

What does that dynamic approach look like?

The static approach where we assessed our information systems every three years has evolved into a near real-time continuous monitoring approach, where we're deploying our security and privacy controls and assessing the effectiveness of those controls on an ongoing basis to make sure that the safeguards are still where they need to be. The fundamentals haven't changed, but we've gone to a much more dynamic and agile way of looking at security—so our customers can obtain greater situational awareness and a better understanding of the security state of their systems on a day-to-day or hour-by hour basis.

We want to ensure that the federal government's operations and assets are well protected; not just when we put those controls in, but over time. The security of our systems must be able to keep up with the modern threats in a world where the attacks can change very rapidly.

How has the security guidance changed over time?

We're growing with the threat space, so to speak. The FISMA Implementation Project is an ongoing initiative. We will never be completely finished

"We want to ensure that the federal government's operations and assets are well protected; not just when we put those controls in, but over time. The security of our systems must be able to keep up with the modern threats in a world where the attacks can change very rapidly."

Ron Ross
Fellow, National Institute of Standards and Technology

with the standards and guidelines because we're living in a world that is so dynamic and where the threats are constantly changing. Organizations hire new people, change facilities and operating environments, bring in new applications, and patch their systems. So there is continuous churn in the IT infrastructure.

If you look at the early versions of the NIST Special Publication 800-53, which is our security control catalog from 2005, you'll see that the number of controls has grown dramatically. We have well over 600 controls now and that reflects the continuing evolution of the threat space and the safeguards we have had to develop for our customers to help counter those threats.

How do you ensure you're creating the right safeguards and countermeasures?

Every one of our publications in the FISMA Implementation Project undergoes a very intense public vetting process to ensure the content is both technically correct and implementable. Everyone gets to see the document before it is finalized, and in some cases, multiple times. We get feedback from individuals and groups within the federal government and from other interested parties in the private sector. We also seek comments from public and private sector organizations around the world.

By the time the document is finalized, everybody has had a chance to look at it and give us their best advice and feedback about what we're about to publish. We use that feedback to develop the highest quality standards and guidance for our customers.

As new technologies such as cloud and mobile solutions emerge, do they present new challenges for your project?

The good news is that the security controls in our catalog are technology and policy neutral for the most part, which means that the controls can be applied to any new technology. Sometimes, however, the security controls have to be adjusted slightly in how they're applied.

For instance, it may be more difficult to scan a smart phone for vulnerabilities on a continuous basis as it can run the battery down. For new paradigms such as cloud computing where you don't have to own your own IT resources any longer, you can provision your resources on demand as the mission or business dictates. That's a little different than the traditional models. But the mechanisms to protect cloud systems are pretty much the same as they are for the non-cloud systems—that is, protecting the computing environment consisting of servers, lots of virtualization, and applications.

This is why the Federal Cloud Computing Program, FedRAMP, uses the NIST Risk Management Framework and the security controls in SP 800-53 to define the cloud protection requirements for the federal government.

What is your top priority going forward?

There's been a lot of discussion about security and privacy controls and how they are implemented within federal information systems. Now, everybody recognizes that in order to really get security to the point where it needs to be, we have to build security in "by design"—that is, building security features into systems and system components early in the system development life cycle.

In many cases, we try to add security features on after the fact, when it is difficult, costly, or impossible to do so. To remedy this situation, we are developing a new security guideline, NIST Special Publication 800-160, Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems. We've been working on the publication for about two years now and the initial public draft is on our web site. In it, we're trying to answer the following question, "How do we use best practices in systems security engineering to help ensure that the systems we build are inherently trustworthy and resilient?"

The analogy that I would use is an automobile. In the early days when you bought a car, pretty much the only safety feature available was a seatbelt. Then over time, new safety features such as airbags were developed. Initially, airbags were optional features but now they are a permanent part of every automobile. So, when you buy a new car today in 2015, you're getting seatbelts, airbags and even steel-reinforced doors in many cases. Those protections are built into the automobile. So, when you get in that car, there are certain things that you, as a customer, don't have to worry about. That's what we're trying to achieve with the SP 800-160—giving customers more confidence in the information systems they use to carry out their critical missions and business operations.

The New Security Model

Cisco provides one of the industry's most comprehensive advanced threat protection portfolios of products and solutions. Our threat-centric and operational approach to security reduces complexity, while providing superior visibility, continuous control, and advanced threat protection across the extended network and the entire attack continuum.

Before, During, and After an Attack

Cisco 2015 Midyear Security Report

Up To 50% Off

For a Limited Time Only

Get Comprehensive Protection

cisco

DEFENDING AGAINST THE ADVANCED MALWARE THREAT

An interview with Steve Caimi, Senior Product Marketing Manager at Cisco

Most data breaches are caused by highly sophisticated malware, which can evade point-in-time detection technologies. Today, more than ever, it is essential for the government to protect its networks with advanced malware protection that augments point-in-time technology with continuous analysis so that any outbreak can be quickly scoped, contained, and remediated.

To learn more about the advanced malware threat and what government can do, as well as other cybersecurity approaches and solutions, GovLoop spoke with Steve Caimi of Cisco.

"Whenever you read about breaches these days, whether it's in the government or outside, typically you'll see the word malware in that write up," Caimi pointed out. "Malware comes in multiple different pieces, they reassemble themselves, they're designed to evade technology that focus on point-in-time type of analysis."

Caimi went on to explain that malware today is designed to exploit all kinds of vulnerabilities that are out there, especially zero day ones that the public sector might not even know about. This malware is designed to understand whether they're being analyzed within a sandbox environment, in which case they could sit there and lie dormant.

Though difficult to deal with, Caimi said there are a number of different types of approaches that the government can take to combat this threat.

"Advanced malware protection must be used," stressed Caimi, "especially those that just don't rely on a given point in time type of a detection. Secondly, you want to be able to contain the malware. If you can see how far that it went, then you certainly don't want it to go any further. And then finally you need to have those capabilities to remediate. A lot of times that remediation has to do with integrating with other types of solutions, so you need to look at that."

Additionally, while advanced malware is a root cause for many data breaches, several (if not most) of the recent government breaches could have been contained or prevented with proper network segmentation security controls, said Caimi. Implementation complexity has been a long-standing issue; properly setting and maintain border firewalls, access control lists, and virtual LAN configurations is a daunting task. But there's no excuse anymore. The network itself – if solutions are chosen wisely – can act as a network segmentation enforcer. And policies can be managed far easier that in the days of old.

"One of the things that we're putting out there is this idea of using the network itself," Caimi said. "So the network itself could be a policy enforcer. And one of the ways that that's done is through technology where you can actually write information about where that network packet can go directly into the packet itself, and then the router and switch, and component technology can enforce that type of policy and do it on a scalable way. So it's another tool in the arsenal and it's a unique Cisco position to do network segmentation, using the network itself as an enforcer."

But no matter how unique or effective your cybersecurity approaches, if they exist in a silo they will not stand the test of time. Cybersecurity solutions that act as information silos simply add complexity and impose higher workloads on already overburdened cybersecurity staff, Caimi said. It's essential to select security solutions that share knowledge and context with other solutions using a platform-based architecture for try knowledge sharing across discrete technologies. This helps the government leverage its existing investments while improving cybersecurity and reducing incident response times.

"I can't stress how important it is to make sure that security information isn't locked in a bunch of silos," Caimi added. "The platform-based type of approaches layer on things like application programming interfaces, using industry standards and so forth in order to make sure that that threat information is shared among different types of technologies."

Caimi said one of the primary reasons it's so important for systems to share knowledge across the board is due to a cybersecurity workforce shortage.

"We can't just throw people at this problem and say, hey, this person is responsible for looking at all the event logs," he continued. "You just can't do that today. There aren't enough people with any kind of cybersecurity experience, especially in public sector, to make that happen. So what is important is making sure that that information is shared across multiple types of technologies and solutions, so you can reduce that complexity."

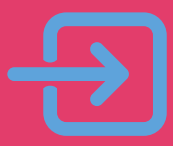
These actions, concluded Caimi, will reduce the time to detection in order to make sure that the public sector can truly stay ahead of all of the threats that are out there today.

WHAT'S NEXT?

The 15 trends in this guide have several common threads, including a focus on collaboration and a need to confront unavoidable insecurity. However, these trends also point to a more powerful conclusion for government: Things can no longer be as they were.

Government cybersecurity can no longer exist in a vacuum, nor can administrators consider government networks the domain of government alone. Instead the experience, functionality, and management of public sector IT must learn from and merge with those aspects of the private sector.

So what does government cybersecurity look like going forward? Here are our predictions for the next phase of innovation in cybersecurity:



THE LOGIN

Just as you can access your Apple iPhone with a touch of your finger, government officials will seek ways to bypass passwords. Expect to see more cognitive and biological login protocols leveraged to streamline and safeguard entry points to government systems.

THE NETWORK

As we connect more devices to more places, people, things, and networks, government and private sector networks will become so intertwined that single-side protection will no longer be enough. It isn't now. As a result, expect to see agencies spending as much time on private partners' cybersecurity technologies and training as they do on their own. In many cases, these tools will be jointly deployed across networks.

THE HUMAN ELEMENT

Every person will become a cyber warrior for government security. Government will find ways to marry private sector interests, such as gaming and mobility, to educate and invest workers in cybersecurity efforts. For government employees, their personal lives will become a greater part of their government digital identity in order to secure organizations from insider threats.

THE SECTORS

Although government and private sector institutions will continue to be legally separate, the cybersecurity of each will be synonymous with the other. Information sharing organizations, procedures, and laws will be created in force to ensure that every level of government is helping every facet of the private market, and vice versa.

THE STRATEGY

Cybersecurity will no longer be relegated to a department, person, or tool. Instead, every facet of a government organization will be ingrained with security by design and consistently monitored for vulnerabilities. To secure constant evolution, efficient private sector collaboration will be crucial. Government will continue to adapt, with cybersecurity at the forefront of every decision.

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 200,000 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
1152 15th street, NW, Suite 800
Washington, DC 20001

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

www.govloop.com
Twitter: @GovLoop

ACKNOWLEDGMENTS

Thank you to Cisco, FireEye, HP, Intel Security, QTS Data Centers, SolarWinds, Symantec, Tanium, Teradata, and ViON for helping us publish this valuable resource.

Authors:

Hannah Moss, Researcher and Writer
Francesca El-Attrash, Editorial Fellow

Designers:

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

Photo Credit:

AC Moraes, Faculty of Medicine NTNU, Elvert Barnes, U.S. Navy, NIST, DHS, DoD, Chris Goldberg, Jonathan Warner, U.S. Marine Corps, Texas State Library and Archives Commission, Samantha Cristoforetti, Tracy Elizabeth, NASA Johnson, Tech Cocktail, Judit Klein, Office of Naval Research, Erik Drost, Fred Moore, Kanaka Menehune, Victor van Werkhooven, U.S. Air Force, ECV-OnTheRoad, Anthony Grieveson.

1152 15th street, NW, Suite 800
Washington, DC 20001

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

www.govloop.com
Twitter: @GovLoop