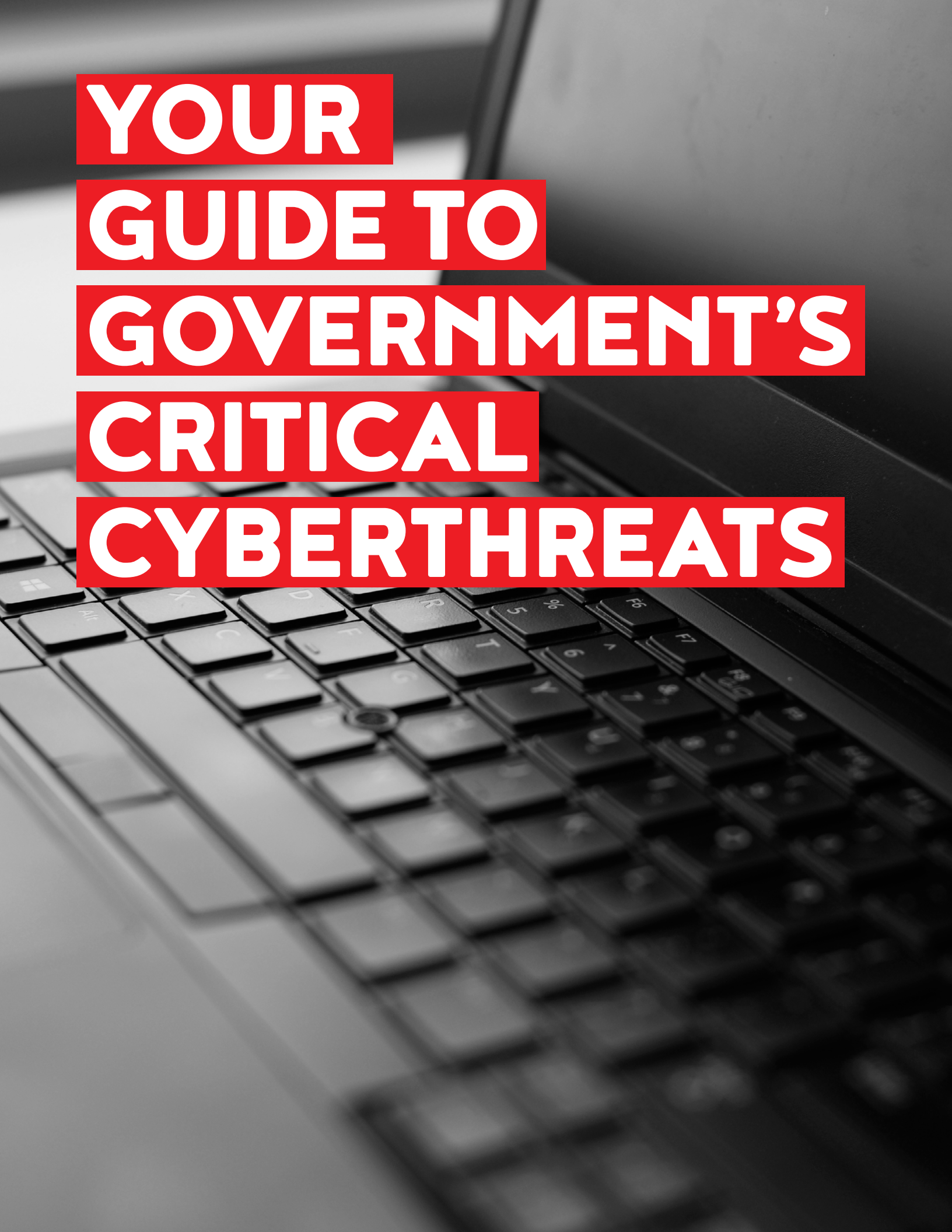


YOUR GUIDE TO GOVERNMENT'S CRITICAL CYBERTHREATS

CONTENTS

TYPES OF CYBERHACKS

INTERVIEWS

INDUSTRY SPOTLIGHTS

IT'S CLEAR THAT GOVERNMENT IS FIGHTING A CONSTANT WAR IN CYBERSPACE, AND IT'S OCCASIONALLY LOSING.

BUT IS THAT THE WHOLE STORY?

HOW GOVERNMENT GETS HACKED

It seems like every time you check the news, you read another alarming headline like "Database leak exposes 191M voter registration records" and "21.5 million exposed in second hack of federal office." It's clear that government is fighting a constant war in cyberspace, and it's occasionally losing. But is that the whole story?

What's often lacking in these attention-grabbing articles is the truth of how government is hacked and what agencies are doing to counter those attacks. Those are the details that are critical to truly understanding the state of government cybersecurity and, more importantly, how agencies can improve their defenses to face future challenges.

In this guide, we'll sidestep blanket terms like "breach" and "leak" to truly explain how internal and external hackers are targeting government information systems.

We will also:

- **Define common tactics**, such as malware, insider threats, and phishing, as well as more sophisticated attacks such as distributed denial of service (DDoS) attacks and advanced persistent threats (APTs).
- **Highlight case studies** of state, local, and government agencies that have endured these cyberattacks and provided countermeasures for future attempts. Relate firsthand perspectives from leading government information security experts.
- **Provide first steps** to better cybersecurity for your agency.

If government is going to fight a war in cyberspace, we must first understand the weapons both sides are deploying. This guide explores the various types of cyberattacks and how we counter them to create a more secure public sector.

A YEAR IN CYBERATTACKS

Because it was exposed in 2015, the 2014 Office of Personnel Management breach captured the most attention in cybersecurity news last year. Yet government endured significantly more cyberattacks across local, state, and federal levels in 2015 than you might have heard about. To give you an idea of both the scale and diversity of attacks that government encounters in a single year, examine this timeline highlighting just a few of the successful hacks against government last year.

January

Jan. 12
U.S. Central Command's (CENTCOM) YouTube and Twitter accounts are defaced by the CyberCaliphate

Jan. 16
A pro-ISIS hacker defaces the website of the Isle of Wight, Virginia

February

Feb. 2
Hackers from 3xp1r3 Cyber Army deface a subdomain of the Arizona Department of Emergency and Military Affairs

Feb. 23
A DDoS attack prevents most New York City officials from sending or receiving messages for nearly a week

March

March 5
Hacktivist group AnonGhost defaces the website of Larimer County, Colorado's Sheriff's Office for the second time in a month

March 7
AnonGhost defaces the office website of the state of Louisiana Rapides Parish Police Jury

March 10
Hacktivisit group, Anonymous, compromises the computer systems of the Madison, Wisconsin Police Department with an apparent DDoS attack

March 23
A Russian hacker disables Maine.gov for about 3 hours via a DDoS attack

May

May 6
A group of Chinese hackers send Trojan-laden phishing emails to the U.S. government, allowing hackers to install plug-ins on victims computers capable of screen captures, folder extractions, and even remote access to computer functions like mouse and click control

May 26
Criminals used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information of more than 334,000 tax accounts through IRS' "Get Transcript" application.

June

June 2
The AnonGhost group defaces the Piatt County, Illinois official website

June 8
Army.mil is taken offline for several hours after hackers, possibly from the Syrian electronic Army, gained access to the website and posted personal messages

June 10
The AnonGhost group defaces two subdomains of the U.S. Air Force

DDoS

ZERO DAY ATTACK

ADVANCED PERSISTENT THREAT

PASSWORD ATTACK

DEFACEMENT

PHISHING

MALWARE

INSIDER THREAT

July

July 1
US-CERT announces detecting a phishing campaign claiming to offer information about the OPM breach

July 10
The Army National Guard announces a breach in cybersecurity after discovering a contract employee inadvertently transferred files with PII of around 850,000 current and former National Guard members to a non-DoD accredited data center

July 10
A pro-Palestinian hacker defaces the official website of New York City's Comptroller

July 25
Upon discovering a cyber breach caused by spear-phishing, the Pentagon Joint Chiefs of Staff's e-mail system for 4,000 employees was taken offline for 2 weeks

September

Sept. 8
Hackers infiltrated the Pentagon food court's computer system, compromising the bank data of an unknown number of employees.

Sept. 16
Trend Micro unveils the details of Operation Iron Tiger, a high-level operation observed stealing trillions of bytes of confidential data from the U.S. government, defense contractors and related companies

October

Oct. 4
The call line of Kennebec County, Maine is targeted with a massive influx of false calls, ultimately disabling the call system

Oct. 14
Bloomberg Business reports that a Russian group continues to target government agencies, including the White House, with repeated hacks

Oct. 15
A number of foreign ministries are hit by a cyber-esponiage campaign leveraging a vulnerability in Adobe Flash

November

Nov. 17
The Department of Interior publicly announces that foreign intelligence agents and other hackers attacked the agency's network 19 times over the past few years to obtain unknown amounts of stolen data

Nov. 22
A collective of pro-ISIS hackers dubbed Team System DZ defaces three domains of the Richland County office

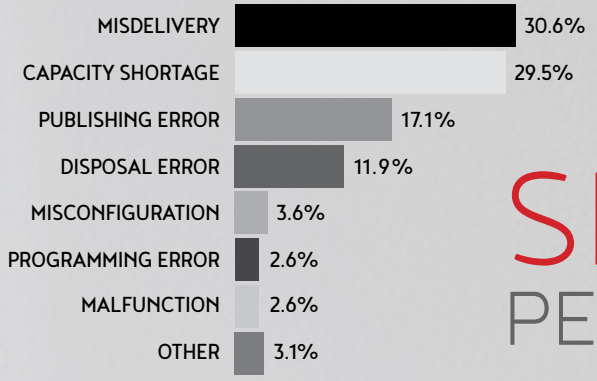
December

Dec. 13
A hacker breaks into the Providence, Rhode Island city website and holds extracted data hostage for 1 bitcoin

Dec. 15
Several online services for the City of Boston are hit by a DDoS attack of unknown origins

INSIDER THREAT

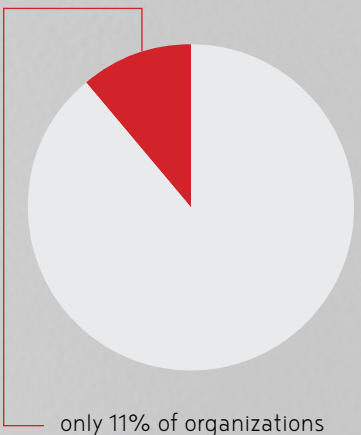
Employee use of government personnel, facilities, information, equipment, or networks of systems to inflict harm on the United States



type of error in 2015 sample of insider threats across industries

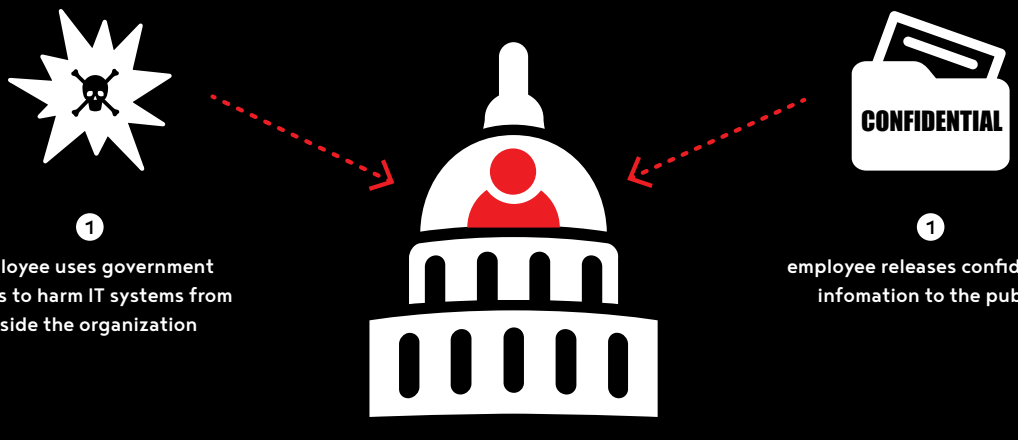
SIXTY PERCENT

of insider incidents were attributed to errors made by system administrators in 2015



only 11% of organizations across industries report feeling totally safe from insider threats

HOW IT HAPPENS:



Livingston County, Michigan Pre-empts Insider Threats

When you're managing a 15-person information technology department, it can be easy to miss indicators of potential insider misuse, especially when you're also focused on keeping the daily functions of your municipality running. That's why supervisors in Livingston County, Mich., installed ObserveIT software to constantly monitor employee use of IT systems and automatically alert managers to potential misuse.

"In a nutshell, it's like a video camera recording everything your employee does on a PC or server. But it's intelligent. It recognizes risky behavior, and it notifies the appropriate personnel when this type of behavior takes place, so it can be mitigated quickly, and you're not waiting 30 months on average," explained the county's Chief Information Officer, Rich Malewicz, in a recent presentation.

In July 2014, that software alerted Malewicz's team to two computers in their treasury and payroll departments that were accessed late at night. It also correlated that access to an employee who had a number of unexplained absences in the near past. Those automated alerts encouraged Malewicz to establish an investigate team and delve deeper into the past online behavior of that employee and others in the department. They used historical data collected by the software and correlated it to other events such as password extractions and data deletions to determine where insider threats might be taking place.

Their investigation uncovered evidence of systems misuse, time theft, copyright infringement, and unauthorized access into some government systems. What's more, they found that not one but four employees were involved in these ongoing incidents.

Before any further damage could be done, the department terminated one worker's employment and the three others resigned. Malewicz attributes his department's ability to quickly identify and eliminate insider threats to their decision to implement continuous monitoring. "Without this evidence, I think those employees would still be here today because they were able to get rid of the physical evidence," he said. "But we had ObserveIT evidence, and you just couldn't deny it."

STEPS TO SECURITY

The FBI provides six tips to help organizations deter insider threats:

1. **Educate** and regularly train employees on security or other protocols.
2. **Ensure** that proprietary information is adequately, if not robustly, protected.
3. **Use** appropriate screening processes to select new employees.
4. **Provide** non-threatening, convenient ways for employees to report suspicions.
5. **Routinely monitor** computer networks for suspicious activity.
6. **Ensure** security (to include computer network security) personnel have the tools they need

DATA SOURCES

Verizon Data Breach Investigations Report (DBIR) 2015
2015 Vormetric Insider Threat Report

Helping agencies transform the business of government.

Alfresco helps eliminate obsolete programs and redundant processes by delivering smart solutions that integrate information and business management processes with compliance automation. Built on open standards and with end users in mind, the Alfresco platform is easy to integrate, simple to use and enables modern, efficient ways of working.

Alfresco helps business owners overcome challenges and solve mission-essential problems by improving performance and program delivery in key business areas including;

- Content Management
- Business Process Management
- Records Management
- Task Management
- Workflow Management
- Digital Evidence Management
- Grants Management

Our Customers Include:

The only open source ECM solution certified to the DoD 5015.02 Standard

Register Now for Content.gov

Learn More on alfresco.com

INDUSTRY SPOTLIGHT

Securing Content in Motion

An interview with Austin Adams, Vice President, Public Sector at Alfresco

Given the abundance and sophistication of cyberthreats, it's inevitable that agencies' information repositories will be targeted and likely breached. But according to Austin Adams, Vice President of Public Sector at Alfresco, that doesn't mean there is no hope for government cybersecurity.

"As long as we accept that as the reality, then we can begin to grapple with solving the problem," Adams said.

That's what his team at Alfresco, a leading provider in content management and security, does – it grapples with the inherent insecurity of government content. But rather than taking the traditional approach of creating robust perimeter defenses, Alfresco creates content-focused security strategies that support agency productivity and collaboration.

Adams explained that content is a critical vulnerability to many government agencies. "When I look at the current layout of most organizations' content, there are significant challenges," he said. "They're swimming in content, much of which is not secure."

He likened many existing content management strategies to an unorganized basement. You aren't quite sure what's in there, whether it's worth keeping, and who has access to it.

SECURITY THROUGH ORGANIZATION

Alfresco helps agencies organize that basement by ensuring that all content is "tagged, secured, searchable, and stored for the appropriate amount of time and in the right places within the enterprise." Rather than trying to hide data behind a perimeter defense, Alfresco's platform enables the agency to organize data and removes any content that isn't necessary to the organization.

This strategy provides two clear benefits to cybersecurity. First, deleting nonessential information minimizes the attack surface by eliminating unnecessary repositories of sensitive information. Second, it allows security professionals to focus on what truly needs to be secured, rather than managing larger expanses of unorganized content.

"We create an organized, clutter-free basement, where you have transparency and a more capable environment to provide security to," said Adams. Alfresco also ensures that retained content is secure by automatically storing it in a secure and organized platform.

Adams cited the Department of Defense task tracking systems as an example of where this automated security is essential. Every task completed by DoD personnel is tracked according to supervisory regulations. Those task orders, which often contain sensitive information, are then recorded and stored.

"Most business process management solutions will say they can do DoD task tracking," Adams said. "But it's an afterthought about where the content is stored, how it's stored, how it's secured, and how you ensure government compliance. That's not an afterthought for us. It's inherently baked into the way that we deliver solutions."

SECURITY WITHOUT SACRIFICING USABILITY

Alfresco's solutions ensure that content is appropriately safeguarded, no matter where it resides in an organization. But while Adams impressed the need to secure content, he also said agencies shouldn't sacrifice content usability or accessibility.

"The way that people thought about security in the past has been about creating that outer wall," he said. "But, I don't know a government agency that doesn't have huge portions of its focus on enabling seamless external collaboration."

Because organizations often share content with external stakeholders, as well as citizens, it doesn't make sense to ensure static security that won't follow content as it leaves the network perimeter. Instead, agencies should ensure security follows content to whatever person or place it is sent, while confirming that access control is appropriately maintained.

"Security should enable content to be shared inside of the context of approved business processes," Adams said. "What we're trying to do is put content in motion, within the context of a business process, while providing security throughout that process."

He offered the example of police digital evidence recordings. Video content from a body or dashboard camera needs to be transmitted from the field to a central repository. Then, it may need to be shared with the justice system or private representation for prosecution purposes.

Securing that content in a traditional content database leaves it open to a variety of vulnerabilities. Alfresco's ability to offer true content management of video and audio ensures that data security and chain of custody are preserved. Doing this at massive scales, in a cloud setting sets Alfresco apart.

Adams concluded, "The goal is to deliver content to the right people at the right time, and to insure that they're getting what they need. No more and no less. And we have to make sure it's secured from the person who creates it to the person who consumes it. Users can't interrupt their business processes to assign security protocols. It has to be built in to the solutions they use."

By applying a security solution that organizes and prioritizes content in a transparent way, and then applies that security throughout the entire associated business process, agencies can empower their content, rather than simply securing it.

PHISHING

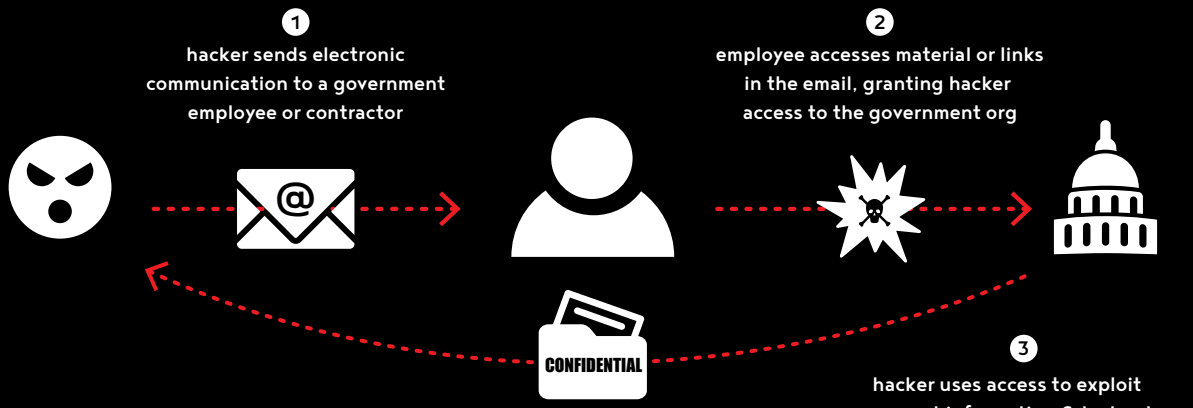
An attempt to extract sensitive information from an individual by masquerading as a trusted entity or person, usually via email or on websites

of recipients opened phishing messages in 2015

of phishing recipients clicked on attachments in 2015

of phishing campaigns that send ≥10 emails are successful with at least one victim

HOW IT HAPPENS:



The U.S. Digital Registry Validates Government Social Accounts

In a recent press release, the General Services Administration's DigitalGov team explained how phishing attacks not only compromise agency security, but can also prevent innovation and decrease citizen trust. "A challenge in embracing emerging startup and private sector platforms for public service is ensuring that citizens can trust the app used for official engagement is managed by the legitimate agency and not an unofficial source, phishing scam or malicious entity," the release states.

Unfortunately, social media accounts and other public-facing government domains can be difficult to identify as valid or false, given that most don't have .gov, .mil, or .us domains.

To enable citizens to confidently access valid government resources while avoiding falsified accounts, DigitalGov created the U.S. Digital Registry in January 2016. The service allows government agencies, programs, and organizations to register any public-facing accounts. That data will constantly update the Federal Government Mobile Apps Directory, a one-stop shop where private citizens can verify the official status of government online services, including websites, mobile applications, and public-facing collaboration accounts.

The registry is still in its early stages, with new accounts being added daily. Ongoing development will be a collaborative effort, in hopes that it will eventually encompass all government public and social accounts while remaining easily navigable by both citizens and internal developers.

Agencies can help by registering their official accounts on MAX.gov. GSA is also working with Facebook, Twitter, and other private social media outlets to consider ways to improve the registry's functionality. Finally, any developer can access the service's code through the Social Mobile Registry or GitHub to "test, evaluate, improve and use it."

Together, these multiple entities will ensure that the U.S. Digital Registry meets its goal of providing a single reference point for all public-facing government domains and social accounts, ultimately minimizing the public's susceptibility to phishing attacks.

STEPS TO SECURITY

Although creating robust spam filters and firewalls can decrease the likelihood of phishing attempts reaching their targets, the best way to protect against these attacks are non-technical, including:

1. **Establishing expectations** regarding online communication to anyone your agency interacts with, including what you will and will not request or send over which channels.
2. **Registering any web domains** or social accounts with the appropriate authorities, including state or federal registries.
3. **Educating employees** and citizen users regarding best practices for identifying phishing attacks.
4. **Formalizing clear channels** to report and communicate phishing attacks in real time to citizens and employees.

DATA SOURCE
| Verizon DBIR 2015

ARLINGTON COUNTY CISO ADDRESSES CYBER WORK-FORCE GAP

DAVID JORDAN
Chief Information Security Officer, Arlington County

State and local agencies face a number of significant challenges in educating, training and recruiting an adequate cyber workforce. There is a clear shortage of qualified personnel to go around. With limited resources, state and local governments have a harder time competing with the private sector to attract qualified cyber professionals to work. Additionally, many elected officials at the state and local levels remain uneducated about their cybersecurity postures, and, therefore, don't advocate for agencies' cyber needs.

Most IT managers at the county level find themselves facing low salaries and huge workloads. Take Arlington County, Va., for example. According to a recent article in Government Technology, Arlington has a population of 250,000 with about 4,500 users on the county network. That network processes some 1 trillion events every day. Yet the county employs just one IT security employee: Chief Information Security Officer David Jordan.

In an interview with GovLoop, Jordan shared his experiences as Arlington County's CISO and insights on needed improvements in the state and local cyber workforce.

CYBER PREPAREDNESS THROUGH CISOs

One of the first things Jordan emphasized was the importance of states having an information security executive position. "The CISO position determines the whole future of the practice," he said. "The CISO determines the quality, education, training, and longevity of the cyber workforce within government."

As the sole IT security staffer at Arlington County, Jordan understands the importance of a well-placed CISO. In the absence of a formal cybersecurity workforce, Jordan meets with all the employees of the organization and regularly briefs IT help-desk workers on issues related to security. He stressed that in addition to being accountable to employees, the CISO should report to the county board or city manager.

"You don't want to have the CISO compete for funding with other leaders within the organization, like the Chief Information Officer," Jordan said. "For many agencies, placing the CISO optimally in your chain of command improves chances of success."

When the CISO does not have visibility or voice within an agency, elected state officials are less likely to promote cybersecurity in their agendas or allocate needed resources for recruiting and training cyber professionals.

CYBERSECURITY THROUGH EVERY EMPLOYEE

Jordan emphasized that everyone who works in an agency has a security component. In Arlington, he combined the power of the county workforce as an extended security operation by enlisting the aid of 4,500 people.

To make sure every employee thinks about cybersecurity, Jordan goes out of his way to talk to every single person who is hired. "Each employee gets me for about 20 or 30 minutes," he said. "We go over the rules of the house and explain the importance of basic IT security. They need to be aware of certain risks and certain best practices."

Jordan established a set of 25 expected behaviors for employees to master in order to promote cybersecurity best practices. He wanted to be available to anyone with questions so he established a phone line. Employees can dial H-E-L-P should they have any questions about potential cyber issues or threats. For example, if an employee gets a suspicious email that could be a potential phishing attack, they can call the hotline to be advised on what to do.

"We also have three chiefs in our IT shop," Jordan said. "We have an architectural design chief, a records management chief, and, myself, a security chief. Once a month, we open our conference line and let people call in and ask questions."

Such methods of communication are efficient ways for cybersecurity leaders to strengthen a team's cyber awareness and preparedness by helping all employees identify any potential scams.

CYBER BEST PRACTICES THROUGH PARTNERSHIPS

In addition to being available to all employees and training his IT staff, Jordan relies on regional partnerships to share information and best practices for cyber training and infrastructure. He collaborates with area peers through a CISO subgroup of the Metropolitan Washington Council of Governments, an independent nonprofit association that brings area leaders together to address major regional issues in D.C., Maryland and Northern Virginia and comprises 22 local governments.

The CISO subgroup communicates daily to share cyber workforce needs, struggles, and best practices. "We can pose questions to each other frequently," Jordan said. "For example, if I'm ordering a new video system for buses, I can send a question to the 22 members and ask if anyone has done this recently or ask about particular vendors they've used."

Regional partnerships are critical for state and local governments when resources are tight, because information sharing can improve cost-effectiveness in cyber training while also developing best practices for any cyber issues.

Through his CISO role, focus on training all employees and regional partnerships, Jordan demonstrates that there is hope for continuing to build the state and local cyber workforce. Having the right staff, such as CISOs, in an agency is critical to setting standards for cybersecurity personnel and infrastructure. Through proper employee education, training, and regional partnerships, state and local governments can have a better chance of harnessing their cyber workforces to better address the cybersecurity needs of today.

TRACK, PURSUE, AND NEUTRALIZE THREATS.

The longer threats remain undetected, the more damaging they become. Take control of your information and fight threats on your terms. It's time to start advancing security.

Take the next step at symantec.com

Symantec™

INDUSTRY SPOTLIGHT

Tackling Insider Threats

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

When it comes to addressing insider threats government still tends to place too much emphasis on user identity, authentication, and authorization. Tackling insider threat doesn't stop at security clearances for each user. There is still a great need to understand if an "approved user" is misusing the data they can access. To learn more, GovLoop recently sat down with Ken Durbin, Unified Security Practice Manager at Symantec, who shared where government is falling short and how authentication and data management can address these shortcomings.

"The problem is strategies stop short on permissions and access to data," said Durbin. "Less emphasis is placed on monitoring users after they are authorized, so they could either inadvertently or maliciously expose the organization's data."

Instead, agencies need to improve data classification and leverage actionable intelligence to better communicate and share information to stop insider threats. Included among Symantec's portfolio of solutions are tools that leverage actionable intelligence and strategies focused on endpoint security, email security, and data loss prevention.

DATA CLASSIFICATION

For government agencies, the first step to better authentication and insider threat prevention is knowing where all data resides so that it can be properly classified. To implement better classification, agencies need to understand where their data is stored, it's level of sensitivity, who is accessing it and why. Durbin suggested solutions like Symantec Data Loss Prevention, which can help prevent the accidental or malicious exfiltration of sensitive data. In addition, they can help agencies:

- **Discover** where data is stored across your endpoints, servers and storage. Identify true data owners and be alerted to unusual activity.
- **Monitor** how data is being used when users are on and off the organization's network.
- **Protect** data by notifying users about policy violations, securing exposed files and folders, and stopping outbound communications.
- **Manage** data loss policies, workflow remediation, reporting, and administration from a web-based management console.

Stronger data classification allows your agency to better detect any unusual activity by your employees. For example, if Joe normally accesses data between 9am-5pm on weekdays, but suddenly starts accessing data at 2am on Sundays, it's critical to have a system that can help you detect that irregular behavior before any sensitive information is compromised.

AUTHENTICATION

The federal government is already implementing multi-factor authentication to strengthen endpoint security. For two-piece authentication, a key chain with a code that changes regularly is used in addition to a password.

While such steps are significant, Durbin suggested that federal agencies take it to the next level: implementing a third-factor of authentication. This is multi-factor authentication that requires a biological component (something you are), like a person's thumbprint, in addition to a user ID and a password. Solutions like Symantec's Validation and ID Protection (VIP) incorporate this third factor into a user's authentication process.

With third-factor authentication, your agency can easily deploy stronger authentication without the expense of deploying and maintaining dedicated on-premises authentication infrastructure. Additionally, this allows for a cloud-based strong authentication service that enables secure access to networks without impacting productivity.

ACTIONABLE INTELLIGENCE

To be effective, these security measures must also be deployed in concert, Durbin explained. "But instead of operating together as an intelligence community, agencies are operating in silos and not communicating with each other," he said.

For example, tools that protect endpoint devices only have information about the endpoint. Likewise, tools that protect network gateways only have information about the network device.

The idea of actionable intelligence is to instead have security tools automatically communicate and share intelligence. With actionable intelligence, potential threats could be identified much faster. "If you could take the information gained from actionable, shared intelligence, it would make your agencies more informed and more efficient," Durbin said.

Tools like Symantec's Advanced Threat Protection (ATP) solution coordinate action at the endpoint, network, and email gateway so that these control points are working together for better overall security against threats, not in silos.

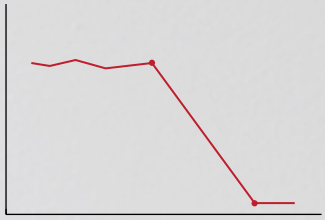
By harnessing actionable intelligence, tools like Symantec's ATP can search for signs of attacks across multiple control points within your agency's infrastructure, all with a click of a button. If you discover a suspicious file in your environment, you can easily retrieve it for further analysis. This is especially important for isolating threats that may compromise your network.

Overall, actionable intelligence provides better communication between your control points, strengthens security, and speeds up your ability to mitigate any potential threats.

It's important to note how far government agencies have progressed in terms of the authentication and authorization processes. However, as Durbin explained, it's just as important to acknowledge when current strategies are falling short. By better understanding data classification, utilizing strategies like third-factor authentication, and harnessing actionable intelligence, agencies can be better prepared to address the challenges that come with increasingly complex cyberthreats.

DEFACEMENT

An attack that alters the appearance and/or messaging of a legitimate website or social media account



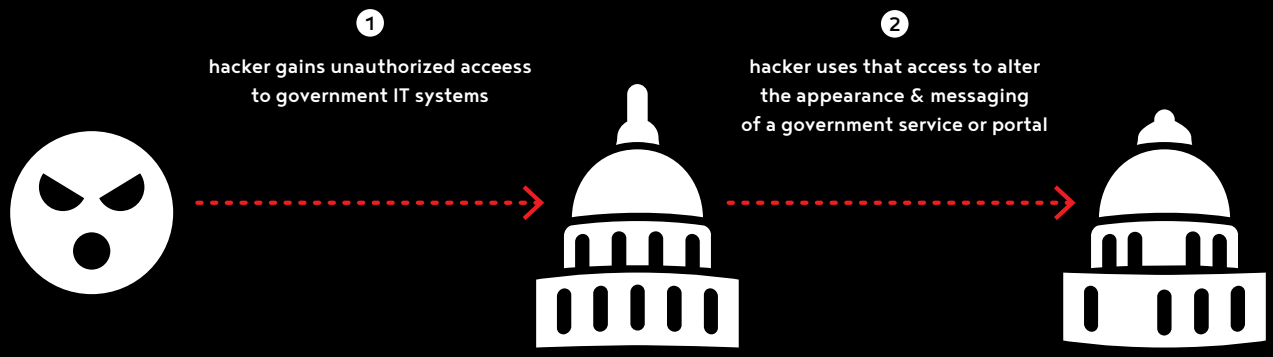
≤95% loss in web traffic if your website is blacklisted by search engines due to defacement

$130
BILLION

in estimated damage caused by a single false tweet on AP's Twitter account, claiming President Obama was injured in a White House explosion

social media accounts linked to the federal government alone

HOW IT HAPPENS:



New Jersey Agency Responds to Website Defacement

The defacement of official government websites and social media accounts may seem like a victimless crime, but these hacks can have real effects on agencies and citizens. Government organizations sacrifice productivity as they attempt to remove false code and imagery. At the same time, citizens may lose confidence in the security or validity of online government services.

On March11, 2015, pro-ISIS hackers breached New Jersey's Casino Reinvestment Development Authority's (CRDA) website. The page normally explains how the agency reinvests funds from the casino tourism industry into state development programs, but many people saw a black screen with white pro-jihad language when they accessed the website last March.

As soon as the defacement was discovered the morning of March 12, CRDA disabled the website for less than an hour to remove the false code.

Although the agency did not prevent the attack, it did take appropriate measures to clearly communicate the breach and its impact to both government authorities and citizens. First, the Newark, N.J., FBI field office, which investigates regional terrorism activities, was notified of the breach. Particularly for a state agency without a robust cybersecurity team, it was critical to share information with more equipped authorities.

Once the website was fully restored, the agency succinctly announced its response and reassured the public, noting, "Immediately upon the brief hacking of our public website this weekend, CRDA staff responded promptly, took the appropriate action and returned the website to its normal functionality. No files or confidential information were compromised."

STEPS TO SECURITY

DigitalGov's Social Media Cyber-Vandalism Toolkit provides several security tactics that can be equally applied to website management systems and social media accounts, including:

1. **Identify** a social media stakeholder team to prevent and respond to cyber-vandalism.
2. **Review** individual application and platform resources so you know what support is available before an incident occurs.
3. **Establish** an internal and external stakeholder rapid outreach plan, including communication templates, to be deployed in the event of a hack.
4. **Review** DigitalGov's Secure Social Media Best Practices Checklist.
5. **Apply** the same security measures, including access control, password restrictions and user education, to social and public accounts as you do to internal, sensitive accounts.
6. **Create** common user responsibility guidance so everyone is clear on expectations regarding public application or platform use.

DATA SOURCES

Paladion
Financial Times
U.S. Social Media Registry

FEDERAL DATA SECURITY BEGINS WITH QTS

QTS Government Solutions™ is the leading provider of compliant managed hosting services for government agencies and businesses.

ABOUT QTS

As a trusted provider of data center, hybrid cloud services and managed hosting, QTS's mission is the 100 percent availability and complete protection of our customers' most important applications and data in a manner that is fully compliant with a superset of federal security standards and other industry-based compliance mandates. Every aspect of our solution – from the facility to the network to the systems we support – is backed by our experience, knowledge and time-tested procedures. QTS also offers VMware vCloud® Government Service provided by Carpathia™ (A QTS Company), an enterprise-class hybrid cloud service delivering VMware capabilities most government organizations are using today, with the added security and compliance assurance of FedRAMP authorization.

- MANAGED SERVICES
- COLOCATION
- CLOUD SERVICES

Visit our website today
qtsdatacenters.com

MORE THAN DATA SOLUTIONS.
DATA SOLVED.

QTS®

INDUSTRY SPOTLIGHT

Achieving Compliance with Multiple Standards

An interview with Kurt Manske, Vice President of Corporate IT & Security at QTS

Agencies have to work diligently to meet with the myriad of compliance standards and requirements, especially during the process of implementing new systems to support updated applications, replace old, aging systems, or implement new functionality. Unless the agency has a strong plan in place for understanding and implementing those requirements, they risk being out of compliance and creating cybersecurity risk for the agency.

In a recent interview, Kurt Manske, Vice President of Corporate IT and Security at QTS, shared how a "one-to-many" approach to aligning with compliance requirements and focus on effective, working relationships with service providers can help agencies better manage compliance requirements while tackling new threats.

ALIGNING RISK WITH COMPLIANCE

Manske recommended thinking beyond just meeting baseline compliance standards. Every organization has a unique risk profile, and the baseline compliance standards must be complemented with efforts specific to the organization risk profile. "Unfortunately, the baseline standards are only part of the effort to secure technologies. Every organization needs to go above and beyond if you want to effectively operate compliant systems – including those in the cloud," he said.

STREAMLINING COMPLIANCE & SECURITY

Every organization should make sure they are streamlining compliance efforts by considering the potentially overlapping requirements within compliance standards.

For example, if a federal agency is required to be compliant with FedRAMP for cloud services, and they also need to be compliant with Payment Card Industry (PCI) requirements because of e-commerce transactions, they need to make an effort to find where the requirements of both standards overlap and implement a single practice that meets both requirements.

Manske suggested that a "one-to-many" compliance approach should be the goal for any organization as it reduces both time to implement and time to manage the compliance efforts.

Agencies should be wary of the subtle differences between the guidelines of disparate standards and make sure that they understand how those standards are interpreted and implemented.

"Many compliance initiatives have some sort of regulatory oversight organization or have a defined set of common standards for expectations as to how the standard is to be adhered to or executed in an IT environment. These standards and expectations are commonly well defined, but they can be unwritten as well. It's important that, as you execute a "one-to-many" approach to regulatory compliance, the agency have a firm grasp of these expectations to know what the set of compliance expectations are. Having a good working relationship with the regulatory agency and/or service provider can help you navigate those challenges."

If an agency doesn't stay on top these differences, it can cause serious noncompliance and security issues. After your organization has a firm grasp of the different regulatory expectations, you will be in much better shape to begin aligning standards in "one-to-many" approach. Your service providers can provide additional counsel for these guidelines

TRANSLATING TO RELATIONSHIPS

Once you have an understanding of your compliance requirements, it's time to translate your needs to your service provider. This won't be a one-time conversation. The reality is cybersecurity threats and practices change over time – even daily.

"It's important that you have an engaged, communicative relationship with your service provider," Manske said. "That way, you can work together to address security issues and threats in real-time."

Manske encouraged asking the following questions internally and having an engaged conversation when considering a service provider relationship for your technology:

- What sort of assurances does your organization have that you're driving security in your day-to-day tasks?
- How do you drive security in what you're doing from an operational perspective?
- How do you drive security in your product development?
- How do you drive security in your project management practices?

The conversation should involve more than just agency leadership. In addition to a technology operational leader engaged in the conversation with the service provider, you should bring in your agency's security leader, audit leader and compliance leader. "An information security leader in the agency needs to have someone at the service provider that he or she can develop a trusting relationship with – someone to have a professional-to-professional discussion regarding security. Same for audit and compliance. These relationships are key to managing risks on behalf of both the organization and provider ends."

Once the conversation is started, keep it going as circumstances change. Communicate the goals and progress of your agency clearly, whether they include moving to a new cloud platform, maintaining compliance requirements or staying on top of ever-evolving cyberthreats.

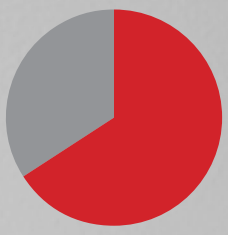
There are many components to managing cyberthreats in the public sector. Navigating compliance standards and requirements should be a top priority, but it's important to remember another critical component: the people and relationships your agency uses to combat evolving cyberthreats. A robust relationship will provide continuous thought and support to both of those components.

PASSWORD ATTACK

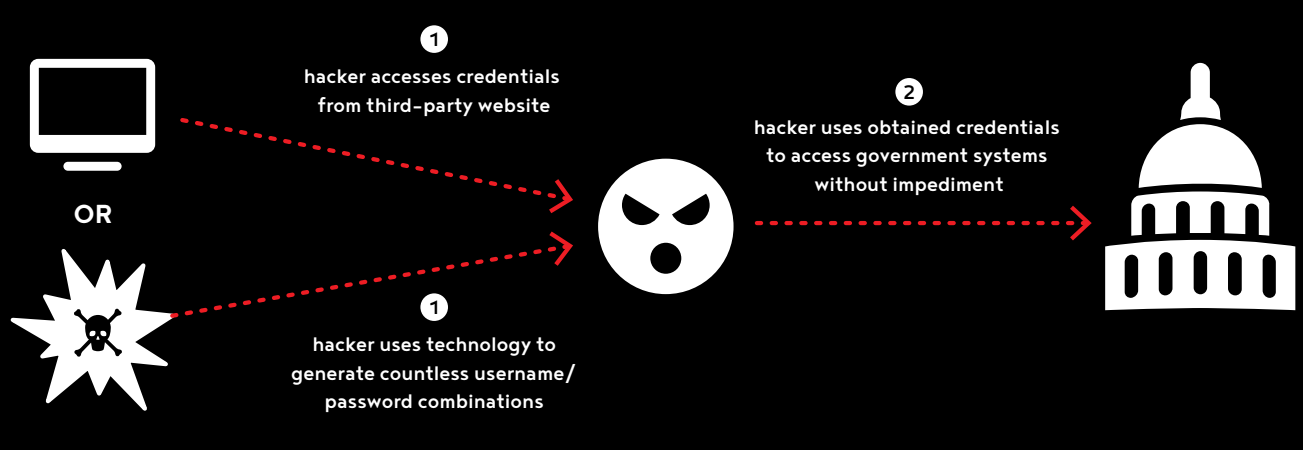
The use of a legitimate user's credentials, including passwords, usernames and other forms of authentication, to fraudulently access secure networks and systems

47 federal agencies' employees' credentials were found accessible on third-party websites in a 2015 investigation

5.6 million fingerprints & 21.5 million social security numbers were stolen in the 2014 OPM breach



2/3 breaches across industries exploit weak or stolen passwords



IRS Allows Hackers to 'Get Transcript'

Occasionally, hackers will obtain secure password information by using brute force attacks on secure systems. That's when they use every imaginable combination of characters, symbols and numbers until one grants them access. In other scenarios, hackers may try to target a secure system's credential system to mine known username/password combinations.

However, both of those scenarios call for hackers to mount technologically sophisticated attacks. That's why it is far more common for hackers to steal credentials from a less secure third-party and use those passwords to target more protected systems.

This last scenario is how attackers were able to infiltrate IRS' "Get Transcript" application in summer 2015. By last August, it was revealed that hackers correlated data from multiple sources to access more than 500,000 taxpayers' accounts. Although some information such as Social Security numbers were reaped from other secure repositories, non-sensitive information such as addresses and marital status were gained from open source locations.

The combined data gave fraudsters enough information to register thousands of people on IRS.gov through the "Get Transcript" application and collect even further confidential material, including former tax returns, from those users.

Following the breach, IRS took the application offline to escape further encroachments using the stolen credentials. In addition, the agency has taken several steps to protect breach victims, including communicating ways their information might be used and offering free credit protection. Finally, IRS will enhance the authentication protocols for the breached application, including assigning existing and new users Identity Protection PINs.

STEPS TO SECURITY

Tight technical security controls are a must for protecting user credentials, but there are also lighter-lift efforts you can undertake to better protect your agency from password attacks:

1. **Educate** employees regarding password creation and protection best practices.
2. **Enforce** strict rules on password construction and protections.
3. **Implement** account lock policies to prevent multiple login attempts (used in brute force attacks).
4. **Require** multifactor authentication on any domains connected to repositories of sensitive information.
5. **Automate** and enforce routine password changes.
6. **Obligate** any third-party contractors to implement the same security controls required of internal systems, leveraging formal security contracting vehicles where possible.

DATA SOURCES

Recorded Future
OPM
Verizon DBIR 2015


SECURITY THREATS
MAY CHANGE, BUT
OUR ABILITY TO STOP
THEM DOES NOT.
As more government data and businesses processes move online, users expect their web experience to be always available and secure.
Akamai helps you safeguard your websites and other Internet-facing applications from the risks of downtime and data theft offering protection against the largest and most sophisticated attacks.
For more information, visit
www.akamai.com/publicsector
Akamai

INDUSTRY SPOTLIGHT

Effective Cyber Strategies for a New Threat Landscape

An interview with Anthony Lauro, Senior Enterprise Security Architect at Akamai

In a recent interview, Anthony Lauro, Senior Enterprise Security Architect at Akamai, a content delivery network and cloud computing services provider, shared how organizations can build new, more effective cybersecurity strategies to combat growing threats.

THE CHANGING CYBER LANDSCAPE

The way we use the Internet has changed. According to Lauro, military sites are an example of this change. Originally, they were primarily used for marketing, but now the sites offer more services, like tracking personnel and providing a customizable user experience. In order to provide those services, the site needs to collect and store identifying data. Today's Internet is a massive network of data warehouses, and attackers aim to access those datasets.

The changing landscape also affects the magnitude of attacks. With the ever-increasing toolset available to hackers, such as malicious stressor sites, DDoS attacks can overwhelm an organization's web services. Another factor is the number of online services to which web systems are connected. Attackers can use valid servers and valid responses as weapons, making it difficult for the target to identify malicious actions.

Organizations' current cyberstrategies are often not enough. One explanation is that it is not economically feasible organizations to build an infrastructure that can withstand massive DDoS attacks without help from a third party. What also leads to the failure of current strategies is the focus on assuming a breach and basing the security strategy around that assumption. Implementing a reactive security strategy does not help reduce attacks in the future.

CREATING A NEW STRATEGY

Instead, Lauro advocated for a forward-facing defensive posture that puts emphasis on offloading traffic and providing a security layer to filter what makes backend services and tools, such as the log correlation servers in the datacenter. By removing the noise that exists within data requests and blocking or validating the requests through several security layers, the backend software can more easily detect threats.

Lauro proposed a strategy focused on three main areas:

Domain Network System (DNS): DNS availability is a major factor in website performance and security. It is important to have a distributed DNS server model, to be able to keep up with new standards, withstand DDoS attacks that aim at taking down this infrastructure, and to answer DNS server requests quickly so the site functions properly.

Web Presence: A website is the face of an organization's digital presence, so reliability is essential. Is the server online? Is it responding to requests? Are the requests trustworthy? How is the site responding to the requests? Going through this checklist using a mixture of network layer and application layer inspection and controls can provide additional security by eliminating potential attacks and dangerous requests.

Infrastructure: Digital infrastructure consists of many parts: the IP address for a router, the server that hosts an organization's mail, and more. It is impossible to hide certain parts of the infrastructure from attackers and still have it be functional, so identifying and rerouting malicious direct to origin requests away from the infrastructure is important or the precious assets that are protected with a cloud based solution could be disrupted if the entire datacenter becomes unavailable.

IMPLEMENTING STRATEGIES & BEST PRACTICES

Akamai's security platform addresses these three areas. The platform takes inbound traffic and redirects it to scrubbing centers, where bad traffic is cleaned and attacks mitigated and good traffic is sent back to the client with minimal delays. This multi perimeter model protects the DNS and the website, as well as the infrastructure. By creating a forward facing security posture and collecting information on attacks, organizations can learn to identify and validate users and requests before they reach the site.

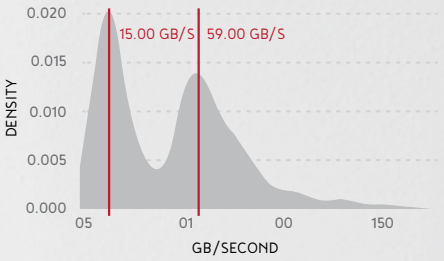
For organizations revamping their own strategies, Lauro recommended following a security framework that defines current organizational needs, future goals, and strategies for improvement and assessment. According to Lauro, successful cybersecurity strategies need three parts: "Understanding how are you going to maintain service under theoretical attack types; training your teams to identify the nuances of these different emerging threats; and looking at the external dependencies that your organization has."

Organizations should also have a set of best practices to guide their strategies. Lauro cited the U.S. Computer Emergency Readiness Team's cybersecurity framework and cyber resiliency review as starting points for developing best practices. These documents break down the lifecycle of a cyberstrategy into five functions: identify, protect, detect, respond, and recover. Each function has guidelines organizations can adapt and implement, such as mapping data flows, training users, and updating strategies.

Despite the rapidly changing cyber landscape, Lauro shared good news: "By following basic practices and sticking to them religiously, organizations can raise their security posture quite a bit." Building a forward-facing security strategy, and developing a set of best practices, like asset management, secure development process and regular training, can help organizations tackle growing cyber threats.

DISTRIBUTED DENIAL OF SERVICE

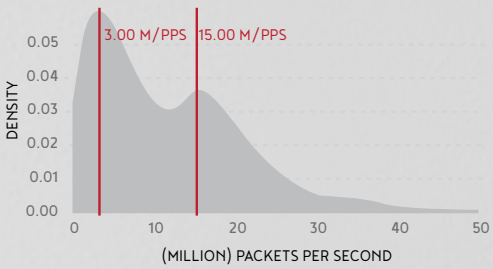
An interruption of network service, executed by sending such high volumes of traffic or data to a single network that it becomes overloaded, resulting in the targeted organization being unable to continue service



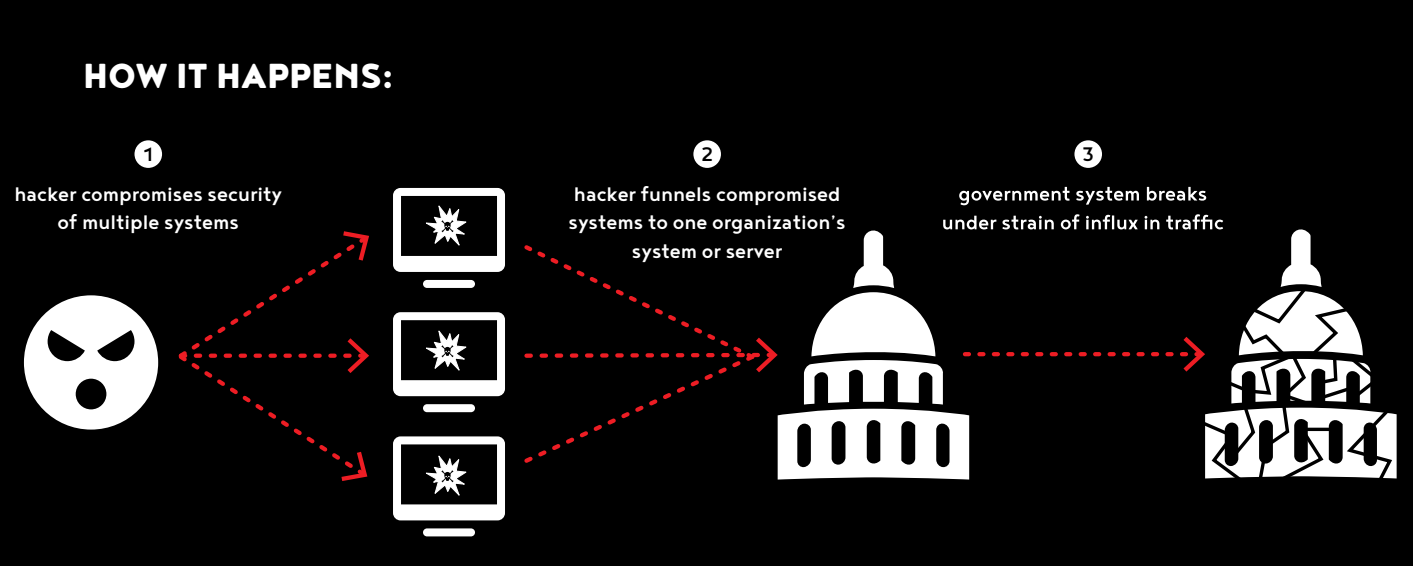
average gigabit load of DDoS attacks

4.5

average number of DDoS attacks endured by a single organization each month



average packet load of DDoS attacks



DARPA's Extreme DDoS Defense

Typically, IT shops attempt to prevent DDoS attacks by combining several tactics, including traffic diversion, network-based filtering, and data replication to dilute attack surfaces. Unfortunately, those tactics often fall short both in preventing low-level attacks, which are more difficult to identify than high-volume attacks, and providing a response plan when attacks break through traffic filters. In September 2015, the Defense Advanced Research Projects Agency (DARPA) announced that it planned to tackle DDoS attacks more holistically with its Extreme DDoS Defense (XD3) program.

According to DARPA's program information, XD3 will take a three-pronged approach to battling DDoS attacks by focusing on:

1. **Dispersing** cyber assets (physically and/or logically) to complicate adversarial targeting.
2. **Disguising** the characteristics and behaviors of those assets through networked maneuver to confuse or deceive the adversary.
3. **Using** adaptive mitigation techniques on endpoints (e.g., mission-critical servers) to blunt the effects of attacks that succeed in penetrating other defensive measures.

As a first step, the agency requested proposals that focused on these three objectives via one of five technical areas, including technology integration, adaptive endpoint sense and response, and networked maneuvering. However, DARPA was clear that it would not consider proposals that focus on techniques to detect malware or trace attacks back to their original hosts.

Ultimately, DARPA hopes to use new technologies and algorithms to create more resilient networks that can better prevent and withstand a variety of DDoS attacks. With a tentative start date of April 1, 2016, the program's goal is to be able to recover a network from a DDoS attack in no more than 10 seconds.

DATA SOURCES
Verizon DBIR 2015
Corero Network Security

STEPS TO SECURITY

US-CERT suggests the following three tactics to prevent attackers from using your computer to attack other computers, inside or outside your agency:

1. **Install and maintain** antivirus software to inspect internal traffic and software.
2. **Install a firewall** and configure it to restrict traffic coming into and leaving your computer.
3. **Follow good security practices** for distributing your email address. Applying email filters may help you manage unwanted traffic.

Unfortunately, it is especially difficult to prevent DDoS attacks because they usually manifest as a simple, albeit massive, influx in traffic. However, you can take steps to prepare your website and services to handle that rapid increase, including:

1. **Deploying perimeter defenses** that inspect network traffic. These tools range from simple firewalls to specific DDoS mitigation appliances that can silo or block suspicious traffic.
2. **Creating "breathing room"** in your IT infrastructure by allocating more Internet bandwidth to your operations than is consumed during routine activity.
3. **Preparing a communication plan** to internal and external stakeholders in the event of disrupted service.

COOK COUNTY TAKES AN ORGANIZATIONAL APPROACH TO CYBERSECURITY

RICARDO LAFOSSE
Chief Information Security Officer, Cook County, Illinois

It's hard to imagine that just a few years ago Cook County, Ill., — the second most populous county in the country — had no centralized management strategy or directive for its various agencies' IT security protocols and tools. Today, the county has both a central security office within its Department of Homeland Security and Emergency Management and a formal ordinance to direct cybersecurity processes across the entire municipality's government, thanks in large part to the county's Chief Information Security Officer, Ricardo Lafosse.

Lafosse joined Cook County's government in 2013 with the primary objective of creating a central information security office, under the leadership of Cook County Board President Toni Preckwinkle. Historically, separate entities, such as the County Clerk or the President's Office, installed and used different tools with different levels of security, despite sharing the same underlying IT infrastructure. "It was a lot of ad hoc, decentralized efforts to do very niche security things," Lafosse said.

That was a significant problem because a vulnerability in one solution could put the entire system at risk, without any other department having knowledge of the risk or an overarching response plan to execute in the incident of a breach. Lafosse was hired to correct that problem.

CREATING CENTRALIZED IT SECURITY MANAGEMENT

Rather than starting with a formal plan, laden with details and protocols, Lafosse decided to begin by addressing the culture surrounding IT. "Cybersecurity is less complicated off paper than on," he explained. "The second you put it on paper, then you have to always follow those procedures. So when you first come on board to an organization that has had no structure at all, you have to ebb and flow with the culture, and then solidify it."

Once Lafosse had a good idea of the county culture, he began making more procedural changes that would improve but not disrupt current processes. In less than three years, his office has made tremendous progress.

"We've centralized a lot of the information security governance structure into a working group," he said. "And now we have a significant amount of security tools and controls in place. For example, we have centralized endpoint management, advanced endpoint management and advanced malware protection."

The centralized organization has also given his office greater understanding of what occurs in their networks. Lafosse said they now know what baseline, normal network behavior looks like, so they can quickly identify and act on abnormalities. They have also created an incident response plan, in the case that abnormal behavior is actually malicious code or another hack in progress.

In addition to establishing these organization-wide tools and plans, Lafosse has created a governance structure to safeguard the county's future IT plan. "A lot of what we deal with are new projects and ongoing projects to ensure that the proper security controls are in place before they get on the network or become production use," he said.

Now, the information security office must review the security implications and give approval for any IT project in the county, before it is deployed. "Doing that, we reduce the need to go back and plug security holes after something goes into production. If we proactively

bake in a lot of the security, it makes our lives and the county's security posture much better from the get-go."

CODIFYING PROGRESS WITH AN INFORMATION SECURITY ORDINANCE

Despite the benefits of these initiatives, Lafosse said it was no easy task to get everyone onboard with these improvements. Many departments, offices, and elected leaders were used to their own tools and procedures, which they could choose and deploy without impediment. To help get everyone on the same page, Lafosse and his team decided to create an ordinance that outlined their office's initiatives, oversight, and expectations regarding cybersecurity.

The ordinance also required each elected official's office to designate a security liaison who would work with the central information security office on incidents, strategy, operations and awareness. That way, "everyone would be accountable from an information security perspective," Lafosse said. "It gives them more skin in the game so that if they lack security controls, we can help them, but if they decide to neglect it, everyone's infected. So that provides, again, incentives to implement security controls."

For those agencies that were already on board with the new central management plan, the ordinance gave them a formal structure for working with Lafosse and his team. It established an Information Security Working Group, which meets monthly to discuss any ongoing or new issues and create more advanced security policies.

LOOKING TOWARD A MORE SECURE FUTURE

Now that Cook County has a centralized cybersecurity structure and policy, Lafosse is looking for new ways to enhance the county's security. He offered a glimpse of his priorities in 2016:

- **Hire more cyber staff.** By changing job descriptions and opening some requirements, Lafosse hopes to recruit more talent to his office.
- **Automate compliance controls.** Using various cloud-based web solutions, the security team will be able to collaborate with vendors on new projects and automatically check products for security and risk compliance.
- **Identify at-risk assets.** Lafosse said they want to assume a risk-based approach to security decisions by identifying their most sensitive assets and applying controls accordingly.

Ultimately, Lafosse said he wants to make Cook County's information security policies a standard that others can emulate. "People look up to us. We're trying to create a framework that other counties can use to quick start their information security office program, which would be very helpful for smaller agencies or other, local or state governments that want to move forward with this type of model," he said.

That goal is certainly a worthy one, not only for altruism's sake but for Cook County's as well. "If more counties are secure as a whole, the entire vertical — every county and every person — benefits," Lafosse said.

Arming agencies with the solutions to securely deliver mission-critical services.

The cyber-defense tool kit to empower your team:

- Advanced Threat Defense
- Malware Analysis
- Anti-Malware
- Threat Intelligence

Learn how to detect and disrupt network attacks at **ThreatTrack.com/Gov.**

ThreatTrack®

INDUSTRY SPOTLIGHT

Three Key Attributes to Make the Most of Your Cyber Data

An interview with Usman Choudhary, Chief Product Officer at ThreatTrack Security

"I've got lots of data but I don't have any context around it. I'm just being swarmed by data." That's a statement that Usman Choudhary, Chief Product Officer at ThreatTrack Security, said he hears often when he talks to cybersecurity teams at government organizations. While agencies are accruing multiple tools to monitor their infrastructures, making sense of the cyber data continues to be a challenge.

"The more solutions and layers they put in place to protect the enterprise certainly generates a lot of opportunity, but often that data ends up in silos," he explained. "Then, being able to leverage that data in any sort of meaningful way becomes difficult."

In order to reap the benefits of this cyber data, Choudhary said organizations should seek three key attributes: context, integration, and value.

CONTEXTUALIZING DATA

While agencies are deploying multiple systems to monitor separate information security functions, Choudhary impressed the need to look at any threat data within the context of your larger IT environment. That broader view allows you to establish baselines, identify patterns, and recognize inconsistencies that might indicate a threat within your system.

Moreover, Choudhary said cyber data must be contextualized within the service you are trying to perform. Having an understanding of how processes and the data they create feed into operations offers a more holistic understanding of individual events. That perspective also helps you prepare a more intelligent threat response that is cognizant of organizationwide implications.

For many agency workers, this contextualization can be a challenge as individual operations teams manage disparate tasks throughout an organization. In those cases, it's helpful to seek tools that help provide context to your larger IT and service environment. "At ThreatTrack, we have made the effort to translate from lower level parameters to higher-level concepts," Choudhary said. That way, even niche teams can act in concert with organizational processes and goals.

INTEGRATING ACROSS SILOES

Once you've taken a holistic view of your environment, it's necessary to extend that perspective to the technical level. "So the good news is that with many of these systems in place, showing us all of these individual threats and events, they provide some context of what's happening," Choudhary said. "But the bad news is that they're still disparate. There is really no knowledge from one system to the other."

To remedy that problem, data siloes and the tools that manage them need to be better connected. "We've really started to see the notion of security analytics, but you can't harness the power of that unless you are truly integrated," Choudhary continued.

ThreatTrack provides multiple security tools in a single package, and integrates those tools across the enterprise. As Choudhary explained, "We wanted to put everything – malware expertise, a strong data science pedigree, and automation, and more – into a single box. While other solutions will identify errors, they'll tell you one thing that you still have to piece together with other tools. We're painting a more holistic view."

IDENTIFYING VALUABLE INFORMATION

This integration also provides the additional benefit of helping organizations identify which data, and specifically which threat alerts, are most valuable. As organizations accrue more tools and therefore more information about their networks, Choudhary said it's easy for them feel as if they're drowning in data without a clue as to which alerts should be concerning and which should be ignored.

For organizations that face innumerable real and perceived threats each day, it's necessary to employ tools that can automatically contextualize your data and identify which alerts are actionable. What's more, those tools should allow you to quickly understand what those alerts mean and which actions should be taken to address them.

Choudhary explained that ThreatTrack identifies and synthesizes multiple security concerns, in order to highlight only the most meaningful information. "We're focusing a lot more on the end user, and bringing to surface things that would take hours or days to identify. We're bringing them to your attention in minutes or seconds," he said.

While organizations will inevitably accrue multiple security solutions to counter the myriad threats facing government, you can avoid getting bogged down in cyber data.

"Yes, you need more data," concluded Choudhary. "But it has to be contextualized, it has to be more integrated, and it has to be high value." To achieve those goals, seek tools that can ease your data burden and provide more insight into your cybersecurity operations.

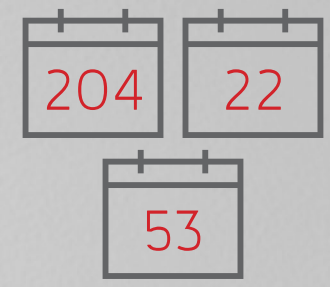
ZERO-DAY ATTACK

Exploitation of an unknown vulnerability in software or hardware to instantly enter a platform or system without impediment

99.9 PERCENT

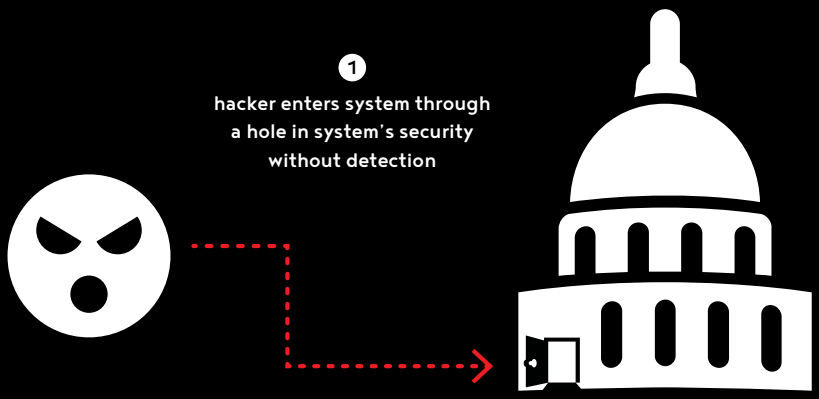
of exploited vulnerabilities are compromised >1 year after the security patch is published

zero-day vulnerabilities, annual total, 2006–2014



total days for vendors to provide patch for top-three most exploited zero-day vulnerabilities in 2014

HOW IT HAPPENS:



DHS Targets Encryption Bugs

Just last year, unauthorized code allowed attackers to invisibly decrypt communications through widely used Juniper Networks firewalls. Juniper sells computer network equipment and routers to big companies and to U.S. government clients such as DoD, FBI, and the Justice and Treasury departments. The breach, also known as the Juniper emergency, took at least three years to be detected, and it wasn't disclosed until Dec. 17, 2015. The Department of Homeland Security (DHS), along with other federal agencies, took the lead in incident response and is currently working to remove listening posts in software planted by suspected cyber spies.

To get to the root of the problem, DHS had to scour its IT inventory to identify affected Juniper systems and any information that ever touched a Juniper firewall. Luckily, DHS, which oversees civilian cybersecurity, has several tools at its disposal to spur agency action. One is the powers entrusted to the agency through the Federal Information Security Modernization Act of 2014. Under it, DHS can issue binding operational directives to help launch better offensive and defensive systems against zero-day attacks. Like many other government agencies, DHS is still looking to stay on the offensive against zero-day attacks in the future.

Today, DHS continues to work with Juniper to assess the risk the compromise poses to government systems and how the Juniper source code was altered. As the agency continues its investigation, it will use its network with other government agencies and private companies to address zero-day vulnerabilities.

STEPS TO SECURITY

The key to preventing future zero-day attacks is improving detection techniques:

1. **Use top-rated security software.** This includes security software that doesn't just cover known threats but also unknown threats.
2. **Update software.** Update your software regularly because most software updates contain security measures against any intrusion.
3. **Update browsers frequently** to make sure they have the latest vulnerability patches.
4. **Establish security best practices**. Set an example of personal online security best practices at your agencies and have your employees do the same.

DATA SOURCES

Verizon DBIR 2015
Symantec Internet Security Threat Report

solarwinds DLT

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


Secure FTP Server


Secure Managed File Transfer

To view the full results of the 2016 SolarWinds Federal Cybersecurity Survey go to: go.solarwinds.com/2016CybersecuritySurvey

IT Management & Monitoring Solutions for Government

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

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

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

Addressing Human Error to Improve Security

An interview with Mav Turner, Director of Product Strategy at SolarWinds

In a recent survey conducted by independent research vendor Market Connections on behalf of SolarWinds, 44 percent of respondents said that the increased sophistication in threats was the primary reason agencies are becoming more vulnerable to cyberattacks. An additional 26 percent cited a sheer increase in volume as a top concerning factor.

Mav Turner, Director of Product Strategy at SolarWinds, explained how to wade through those mounting threats to achieve better security. "First, you have to consider who is the attacker? You should have clearly defined defenses deployed to protect against internal and external attackers. Second is the how. What are the specific types of attacks that you are most vulnerable to and do you have appropriate prevention and detection strategies in place," he said.

KNOW THE SOURCE OF YOUR THREAT

Regarding sources, Turner particularly separated external and insider threats and said it's important to identify which is most likely to expose your organization. While we commonly think of external attackers as the main instigator of breaches, SolarWinds' survey found that 68 percent of IT professionals reported security breaches caused by human error and an additional 25 percent of respondents reported privileged access abuse by organization employees.

Internal attackers often have privileged access to systems that they can take advantage of. Also, internal users have access to confidential data as part of their job. Ideally that data would never leave the direct ownership of the agency, but with mobile devices more prevalent than ever, it's very difficult to ensure sensitive data doesn't get out.

"The trick is always to look at the concerns for you specific agency," Turner said. "IT Pros need to understand what services and what systems they have, how they operate, and who uses them."

ADDRESS INSIDER THREATS WITH TOOLS AND TRAINING

Once you identify the internal or external threats that your agency is most susceptible to, it's time to apply solutions. "With the combination of tools and investment in people, you can help address many of the human errors," said Turner.

It begins with training. Especially as agencies accrue new solutions, the need for training becomes more crucial. "As the complexity of an environment increases and you bring in new technologies like cloud or software-defined networking, and as those technologies become critical to the infrastructure, human error increases because workers don't have the training to manage these systems," Turner said.

While most organizations know that education can greatly reduce the risk of human error, it is rarely delivered effectively. Turner cited the tendency to prioritize operations over security, as well as time constraints on IT staff as major barriers to success. To overcome those barriers, agencies should consider complimenting training with effective technology suites.

While insider attacks often abuse weaknesses in process and training of other employees, Turner said you shouldn't discount technical solutions that can help mitigate human errors. Particularly, automated processes can create safeguards in processes and free time for IT staff to focus on security.

"For instance, products that automate network configuration management can require multiple parties to approve any one change. So before anyone makes a change to the infrastructure, someone else has to look at it and determine if it could create a vulnerability" he explained. That way, even if one person does make a mistake, the tool will help ensure it is noticed before the change is released.

Automated patch management tools can also minimize the potential of human error by automatically repairing vulnerabilities in 3rd party software before an employee can accidentally be tricked into running something that abuses that flaw to execute an attack. That automated patch deployment also saves IT staff valuable time, allowing them to focus less on everyday operations and more on advanced security efforts.

"Automation is absolutely critical to any security team," Turner continued. "The other necessity is tighter integration between operations and security."

Performance management tools can provide greater transparency into the operations of your systems, as well as abnormal activity that might point to an attack or breach. "So all the performance monitoring tools actually help provide the visibility to improve security and it helps bring together operational and security teams in the process," Turner said.

SECURITY TO DELIVER BETTER SERVICE

Finally, Turner explained how investing in training and tools to mitigate human errors can ultimately lead to better government. "If you have the right people, process, and tools in place to operate efficiently, in addition to improving security, you're also likely delivering better service," he concluded. "When IT has a problem, the whole agency has a problem. But by making sure you're applying the right resources and decreasing human error, agencies can focus on their mission, rather than worrying about the tools they are using to accomplish that mission."

MALWARE

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

96 PERCENT

of mobile malware was targeted at the Android platform between January and October 2014

$200 - $10000

the typical ransom fee an organization must pay a hacker to have them remove ransomware from internal systems

95%

of malware is present for less than a month. 4/5 malwares don't last for more than a week

HOW IT HAPPENS:

Ransomware Wins in Maine Towns

When you think of malware, you probably think of the simplest type of code-based hack that corrupts your computer or destroys information. However, malware can be much more sophisticated than that. One type of complex malware that has proven particularly troublesome for government is ransomware.

Ransomware, as you might expect from the name, is a type of malware that extracts or blocks information from a system until a fee is paid to the author for its return. For state and local agencies, this type of malware is difficult to effectively combat because it can be deployed through several channels. What's more, it's often costlier to internally remove ransomware than to simply pay a small fee to the hijacker to release your data.

When the Lincoln County Sherriff's Office — and four other towns in Maine — were hit with ransomware in April 2015, they faced that choice. A hacker contacted the office after rendering the computer system unusable and threatened to delete all of its data if ransom wasn't paid.

The decision became whether to invest more money in hiring someone to safeguard the system in a timely manner or give in to the hacker's demands. Because the requested fee was only $300 — a small sum in the scale of a county's IT budget — the office and adjoining towns decided to pay it.

Once the hacker received the payment, in the form of the online bitcoin currency, the county received a code to unlock the computer system. No data seemed to be altered or extracted.

"We needed our programs to get back online," said a Police Chief from one of the affected towns. "That was a choice we all discussed and took to get back online to get our information."

STEPS TO SECURITY

Because malware can enter your IT system through a wide variety of channels, an effective prevention strategy will necessarily be multifaceted and constantly in need of refreshing. However, these basic FBI tactics will help secure your computers from common malware threats:

1. **Keep your firewalls** on and up-to-date.
2. **Install and update** antivirus software.
3. **Install and update** anti-spyware technology.
4. **Keep operating systems** up-to-date and install all available security patches.
5. **Educate employees** on ways to identify phishing attempts that may carry malware.
6. **Shut down IT systems** and computers when they are not in use.

DATA SOURCES

FireEye
Verizon DBIR 2015
FBI IC3

The future of technology is more secure than ever.

Intel® Security combines the expertise of McAfee® with the performance and trust of Intel to deliver secure computing to consumers and businesses worldwide. We believe that as technology becomes more deeply integrated into life, security must be more deeply integrated into technology. Because when everyone has the confidence to use technology to its full potential they can achieve their full potential. Visit intelsecurity.com.

intel® Security

McAfee is now part of Intel Security.

INDUSTRY SPOTLIGHT

Outcome-based Strategies for Better Cybersecurity

An interview with Ned Miller, Chief Technology Strategist for Public Sector at Intel

Phishing attacks, advanced malware, and ransomware are just a few of the types of cyberattacks that government deals with in today's current cyberthreat landscape.

In an attempt to counter such attacks, many agencies focus on tool-based strategies as cyberthreats come.

But the problem with such approaches is that agencies are usually ill equipped to apply such tools and usually address the problem when it's too late. That's why there's a need for more proactive results-based strategies. In an interview with GovLoop, Ned Miller, Chief Technology Strategist for Public Sector at Intel, shared how agencies can harness better outcome-based strategies to navigate in the current, complicated cyberthreat landscape.

OVERCOMING CYBER CHALLENGES

Intel works to help government agencies achieve their desired state. "The desired outcome for our customers is helping them build a resilient digital enterprise that can withstand sophisticated attack campaigns," he said.

To achieve this desired state, Intel focuses on helping government agencies address four basic criteria:

- **Neutralize emerging threats.** Shift agency tactics from a fire-fighting mentality of addressing the attacks as they come to a strategic lifecycle defense. This prepares an agency to automatically address emerging threats before they become a real issue.
- **Safeguard vital data**. Establish control between end users and advanced capabilities, such as those of the cloud. Safeguarding data means having the ability to control the data and protect it regardless of where your data lives or how it moves between platforms.
- **Fortify critical environments**. Gain comprehensive visibility and create consistent policies across your organization. Be agile in leveraging your resources without sacrificing security when fortifying various environments like datacenters and multiple cloud platforms.
- **Optimize Security Operations.** Harness dynamic control and automation to improve security operations and standards. Develop automated mechanisms to provide more visibility throughout the organization in addition to control, and take advantage of intelligence information in real time to be more proactive.

OUTCOMES BASED STRATEGIES FOR CYBERSECURITY

In addition to adopting these four criteria to achieve your agency's desired state, it's important to look at more holistic and proactive strategies against cyberthreats. As new threats emerge, it's tempting for organizations to acquire more cyber tools, which are often purchased and updated when it's too late to prevent an attack. Additionally, many government infrastructures simply don't support the new tools and organizations, then feel forced to change their current infrastructures to accommodate them.

"This leads to several challenges," Miller said. "One is that we put more stress on security practitioners in the organization because there's a learning curve to the new tools. Additionally, we're not hiring more people to run those tools, and it causes a lot of cyber personnel to feel overburdened."

Instead, Miller suggests better configuration-based compliance checking and being more proactive in security postures. This requires more outcomes-based strategies. Using automation, a message fabric that allows communication in real time, and sharing threat intelligence data allows organizations to react earlier to threat conditions.

Miller suggested a three-pronged approach to implement as a comprehensive outcomes-based strategy:

1. Dynamic control and automation:
Due to the lack of skilled resources and cybersecurity practitioners, government is not producing enough labor and talent to catch up with cybersecurity needs. That's why it's important for organizations to incorporate more automated mechanisms to provide better control and visibility.

2. Contextual risk cognition:
There is greater need to look at the context of cyberrisks in order to perform better behavioral and advanced analysis. Leverage data gleaned from advanced analytics to make better decisions that address your particular cyberthreat landscape.

3. Pervasive points of presence:
Citizens and government employees alike want the ability to work from anywhere, anytime. With the increased demand for connectivity comes increased need for security and better information storage. Pervasive points of presence means enabling mobile technology devices that transmit and share data across the Internet to provide connectivity while ensuring security.

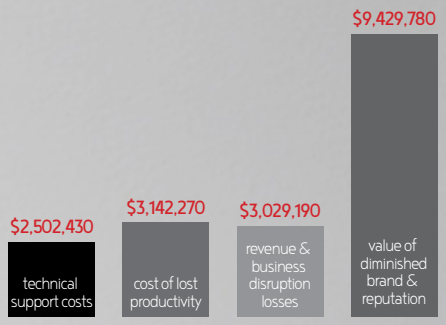
While the cyberthreat landscape has grown larger and more complicated, government should not have to rely on new tools alone to combat new cyberthreats. Instead, leveraging outcomes-based strategies with a focus on automation, risk cognition, and securing mobile data is key to any agency's cybersecurity protocol.

By focusing on results rather than just on new tools, government can better build their cyber workforce and work towards achieving a desired state of resilient digital enterprise.

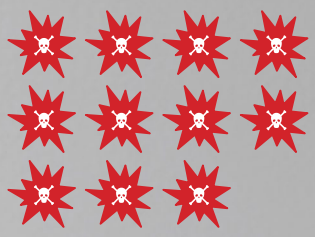
ADVANCED PERSISTENT THREAT

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

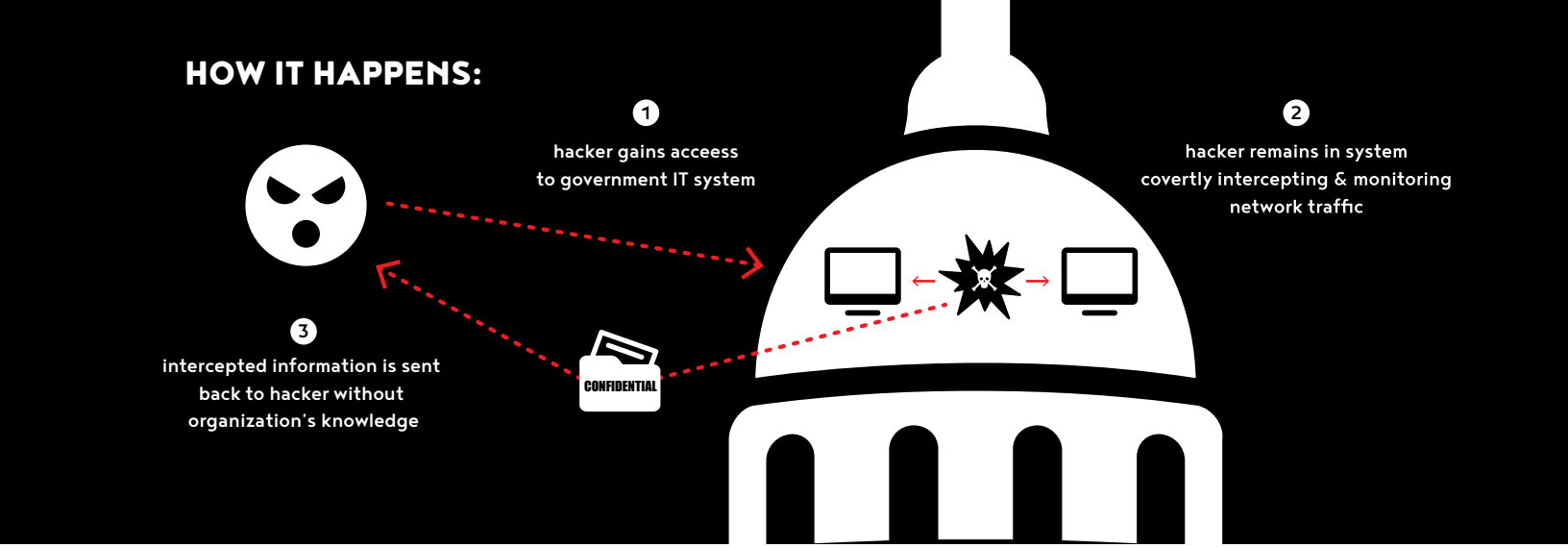
of APTs start with phishing attacks



average costs of APT-related incidents for four categories



11 unique APT attacks per day on average in 2013



A Russian APT Takes on Federal Government

Creating and deploying APTs requires significant time, skill, and other resources. For that reason, they are more common in state-sponsored cyberattacks than in autonomous hacking groups. Specifically Russian and Chinese state-sponsored groups have become adept at deploying these hacks.

In November 2014, a Russian APT group attacked the State Department. The activity was detected in the system concurrently with another cyber-attack that hit the White House computer network.

Then, in the summer of 2015, malware from two Russian hacking groups bombarded U.S. federal agencies. Those waves targeted 2,000 senior officials, including at least one member of Obama's Cabinet, and the personal email accounts of their spouses.

In response to the cyberattacks of 2014, State took the unprecedented step of temporarily shutting down its unclassified email system. However, months later it was evident that the measures didn't fully clear the advanced hack. In March 2015, State again disabled large parts of its network to remove malware from Russian hackers in its unclassified email system. This was the second attempt at repairs from the ongoing cyberattack.

As of 2015, the U.S. government has been increasingly on the lookout for potential attacks from the Russian APT group. The same hackers linked to the attacks against State and the White House were said to have set their sights on the Pentagon. Government agencies and private companies alike are working to step up their cyber tools to detect APTs earlier and better combat potential attacks.

STEPS TO SECURITY

Because common entry points for APT include applications and the humans operating them, it's important to place strong protection around the endpoints and access points into the network. Use these strategies from the SANS Institute to strengthen your agency's protections:

1. **Secure remote access**. Use security access devices such as Secure Sockets Layer Virtual Private Networks.
2. **Check and remediate endpoints**. Endpoint controls can mediate time-of-day access and restrict system access based on remote location.
3. **Use DNS Security Extensions** to provide a cryptographically signed and valid response that represents a chain of trust.
4. **Consider a web application firewall** appliance that protects against web-based vulnerabilities such as buffer overflows and cross-site scripting.

DATA SOURCES

Infosecurity
Ponemon Institute
FireEye

THE COLLABORATIVE FUTURE OF FEDERAL CYBERSECURITY

MARK KNEIDINGER
Director of Federal Network Resilience, Office of Cybersecurity & Communication at DHS

Federal agencies are under increased pressure to effectively secure government IT after a series of headline-making breaches were discovered last year. But in a recent interview, Mark Kneidinger, Director of Federal Network Resilience in the Office of Cybersecurity and Communication at the Department of Homeland Security, said that pressure may be exactly what government needs to move forward.

"That pressure's almost like applying pressure to create a diamond," he said. "You really are creating a very strong unified front now."

Today, government agencies are seeking new ways to work together to create a better cybersecurity. "What we're seeing is really a major sea change that is occurring across agencies in regards to the level and degree of collaboration," said Kneidinger. "They're not seeing themselves as an island unto themselves anymore, but instead realizing the deep dependencies on each other in regards to best practices, as well as shared services."

THE CASE FOR COLLABORATION

Federal government is known for operating in siloes – so why the sudden focus on collaboration?

Kneidinger mentioned the OPM breach that made headlines last year as one reason. "That breach really brought to the forefront that agencies need to know how well prepared they are, so they don't end up the next one on the front page of the newspaper." But he said what really motivated agencies to think more collaboratively about cybersecurity was the federal response to that breach.

Kneidinger cited last year's Executive Memorandum 16-04 and the President's current Cybersecurity National Action Plan (CNAP) as prime examples. "If you look at both those documents, you'll see how agencies are preparing themselves to combat the various cyber incidents by working together," he said.

For instance, the Cybersecurity Strategy and Implementation Plan outlined in Memorandum 16-04 ultimately involved 63 federal agencies, which worked together to achieve seven objectives. The mission of the seven working groups was to provide recommendations for implementation in support of these objectives during a 30-day sprint. "So the driver was the OPM breach," said Kneidinger. "But then these actions were identified that collectively the government worked together in very short sprints to be able to accomplish a great deal."

Additionally, he referenced the binding operational directive (BOD) who authority was provided to DHS through FISMA 2014. The first directive was targeted at identifying and securing critical vulnerabilities across agencies. But Kneidinger impressed that the the most interesting thing about the BOD – beyond the speed which the agencies responded to mitigating the critical vulnerabilities – was the communication norms it established between agency CIOs and deputy secretaries.

"Bringing that visibility to the Deputy Secretary was so important and it provided the CIO a couple things," he explained. "One, it provided the CIO the visibility to the Deputy Secre-

tary on a regular basis that in many instances had not occurred. Two, it gained the support of the Deputy Secretary to support the CIO, in accomplishing his tasks, specifically in the cybersecurity area." These formalized communication channels helped create a more holistic and collaborative approach to cybersecurity among agency leadership.

Kneidinger joked that usually when you release a directive, you're likely to see resistance to the order. However, he's actually seen many leaders thank DHS for enforcing the directive and establishing these channels. "To get a thank you to provide that forcing factor certainly was unusual. But the BOD reemphasized the need of really building and opening that communication channel up between the deputy secretaries and the CIO, and quite honestly, reinforcing that communication channel between the CIO and the CISO."

TACTICS TO BOLSTER COLLABORATION

Kneidinger is excited at the possibilities that collaboration will provide to cybersecurity efforts. "We need to be able to share what we're learning, how we're approaching events, as well as when we take a look at programs, take a look at them from a government-wide perspective."

Nevertheless, he did note a few challenges that might hinder collaborative efforts, skill recruitment and retention being at the top of the list. While collaboration across agencies will certainly create stronger cybersecurity, each team still requires skilled staff to deploy and maintain day-to-day security tactics. "One of the ways that we can do that is provide the cybersecurity professional an opportunity for the growth, for training, to work on critical interesting projects, to provide an opportunity for them actually to move around on different projects and take on short-term projects."

He mentioned the effective recruitment efforts of newer digital agencies like 18F and the US Digital Service as prime examples of how government can attract technical talent with these tactics. "What we're looking at from the CNAP aspect is, how can we replicate these types of approaches in the rest of government," he said.

Second, Kneidinger said that despite the increased awareness of cybersecurity needs across agencies, "there's a broader need in regards to having the mission owners within the agencies understand the criticalness of cybersecurity, and what that means in relationship to the type of data that they own."

To help increase cybersecurity ownership among staff, Kneidinger's team is providing data and educational materials to agency leaders outside the IT suite. He recalled a recent occasion where one agency requested a briefing for all of the commissioners, executives, and secretariat staff regarding what data the agency maintained and how that data – if left unsecured – might compromise the organization and its partners.

After that briefing, Kneidinger said "the light bulb turned on for many executives to realize that 'Okay, I have more of a responsibility in cybersecurity than just saying the CIO and CISO are going to take care of it."

Kneidinger wants to see that awareness continue to expand among government ranks. However, his agency can't do that alone. "Part of the challenge from that expansion perspective is actually the capabilities of the CISO to be able to relate to the mission owners, the importance of what they're doing from a security aspect, and the impact on the mission owner's data."

Yet he said many federal CISOs don't have the same access and authority over agency staff as their CIO partners. So his third main area of focus for collaboration is to help federal government rethink the CISO position – in regards to both authority and ideal skillset – to broaden the relationship between CISO and mission owner.

Finally, Kneidinger impressed the need to overcome the traditionally static nature of government. "We need the general ability to move rampantly in the ever changing environment," he said.

Here, collaboration will be a key to progress. "I think the positive side is that if you have more eyes on the threat issues, and you're sharing more information, you're going be better prepared to identify the threats and catch them in advance," Kneidinger concluded.

LESSONS LEARNED

To give you an understanding of how expansive the cybersecurity landscape is, we've highlighted some disparate types of cyberattacks and the multiple ways government agencies have strategically countered them. But as we described these cyber scenarios, certain commonalities became obvious.

Although there are significant differences among the tactics hackers use to breach government, the lessons agencies learn from those attacks and leverage for future security are consistent. If you compare the case studies in this guide, you'll notice these four priority actions:

SECURE ALL FRONTS.

When you consider the disparate ways the attacks detailed in this guide can enter your network, it's obvious that you can't rely on any single strategy to secure your entire network. Instead, you must safeguard every endpoint, including employee-only gateways and public-facing domains. Moreover, you must deploy a variety of tactics on each of those access points to ensure you're safeguarding against both sophisticated, technical attacks and targeted, behavioral exploitations.

INVEST IN EDUCATION.

You might think of firewalls or spam filters when you think of endpoint security, but your first and best line of defense is your employee. Agencies are most often put at risk by the accidental misuse or exploitation of internal systems by their own staff, as our phishing, insider threat, and other case studies highlighted in this guide. Yet those employees can also be your greatest cyber strength when you train them to securely use your systems and identify potential internal threats. In addition to investing in necessary cybersecurity technologies, be sure to set aside time and resources for employee cyber education.

PLAN FOR THE WORST.

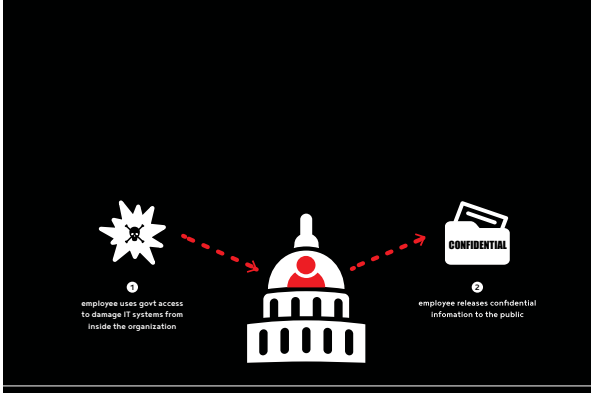
The breached organizations highlighted in this guide all have one key aspect in common: When they were hacked, they responded quickly and publicly. Prevention is ideal, but with the volume and sophistication of cyberattacks today, it's inevitable that something will break through your defense. Craft a plan for countering successful hacks and communicating your response.

DON'T GO IT ALONE.

From both resources and awareness perspectives, it makes sense to share as much of the cybersecurity burden as you can across agencies and levels of government. Local and state authorities can obviously benefit from the support of better-resourced federal agencies. Moreover, federal organizations can mutually benefit from information sharing among levels of government as hackers use the same hacks and tactics for multiple targets. Finally, every agency should seek private partnerships, particularly to secure third-party software and applications that interact with government.

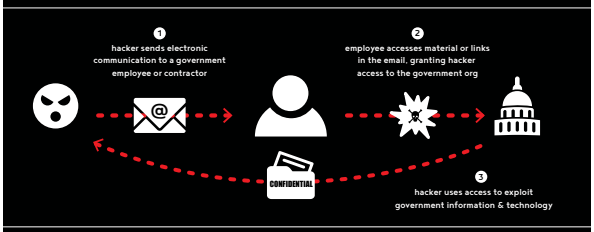
The case studies in this guide exemplify the possibility that government can effectively prevent or counter cyberthreats, even as they multiply in both volume and sophistication. However, the fight for security in cyberspace will be won only if agencies learn from one another and from their previous failures.

APPENDIX



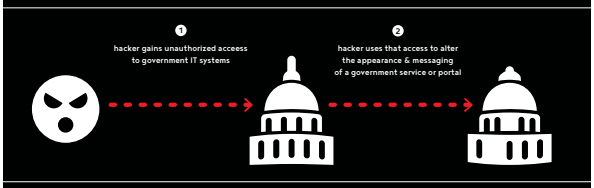
INSIDER THREAT

Employee use of government personnel, facilities, information, equipment, or networks of systems to inflict harm on the United States.



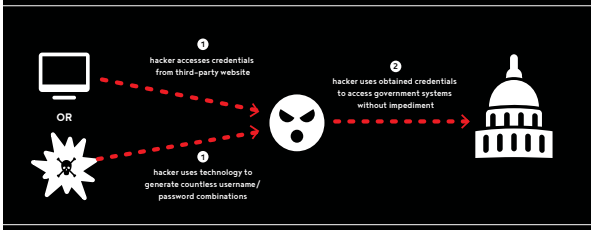
PHISHING

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



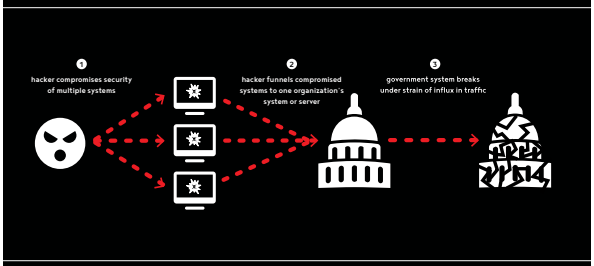
DEFACEMENT

An attack that alters the appearance and/or messaging of a legitimate website or social media account.



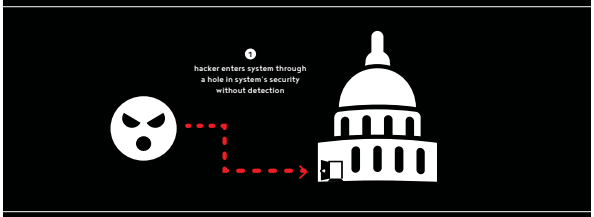
PASSWORD ATTACK

The use of a legitimate user's credentials, including passwords, usernames and other forms of authentication, to fraudulently access secure networks and systems



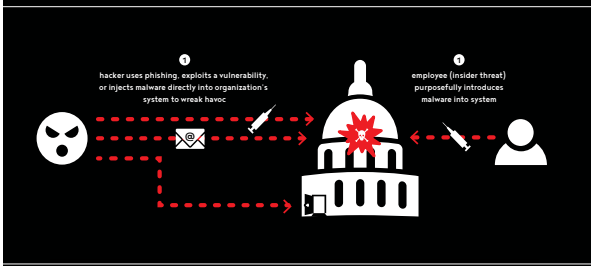
DISTRIBUTED DENIAL OF SERVICE

An interruption of network service, executed by sending such high volumes of traffic or data to a single network that it becomes overloaded, resulting in the targeted organization being unable to continue service.



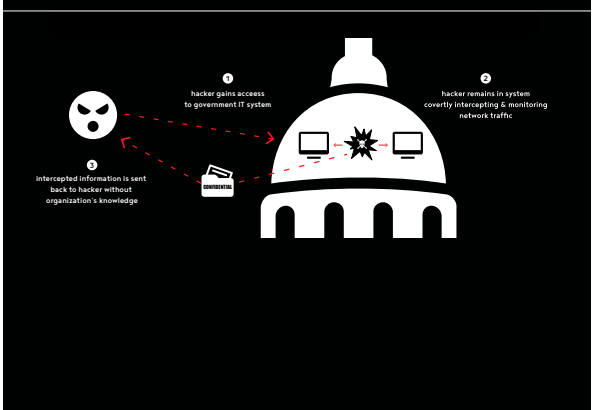
ZERO-DAY ATTACK

Exploitation of an unknown vulnerability in software or hardware to instantly enter a platform or system without impediment.



MALWARE

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



ADVANCED PERSISTENT THREAT

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

ACKNOWLEDGMENTS

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 250,000 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.

www.govloop.com | @GovLoop

THANK YOU

Thank you to Akamai, Alfresco, DLT, Intel Security, ThreatTrack, QTS Data Centers, SolarWinds and Symantec for their support of this valuable resource for public-sector professionals.

AUTHORS

Hannah Moss, Senior Editor & Project Manager
Francesca El-Attrash, Editorial Fellow

DESIGNERS

Jeff Ribeira, Creative Manager
Tommy Bowen, Graphic Designer
Kaitlyn Baker, Junior Designer
Martin Nera, Junior Designer

1152 15th Street NW, Suite 800
Washington, DC 20005
P: 202.407.7421 | F: 202.407.7501
www.govloop.com
@GovLoop