Understanding the Dangers to Your Cybersecurity

govloop

Table of Contents

Executive Summary

Imagine that your agency has suffered a cyberattack. Embarrassing headlines about your organization's cybersecurity appear daily, and citizens are outraged that their sensitive data isn't safe. Whether your agency is federal, state or local, it's a nightmare that can come without warning.

Unfortunately, there's no way to protect your organization from cyberthreats permanently. Today's cyberthreats are constantly evolving, and the danger they present never fully disappears.

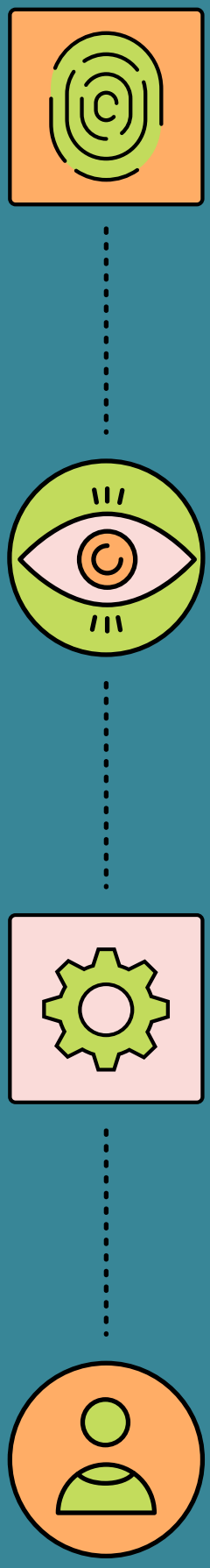
Still, the pressure is on agencies to defend themselves by quickly detecting and minimizing security risks. The consequences of failure are severe: These events drain agencies' energy, money and time. Even worse, they can hurt your organization's reputation or endanger national security.

Protecting citizen data is difficult, however, when you don't understand the cybersecurity world around you. Agencies that aren't familiar with the latest threats won't see the attacks coming at them. That puts both citizen and public-sector data at risk.

The danger to agencies will only grow as cyberthreats adapt and evolve. For example, National Security Agency (NSA) official Rob Joyce said in December 2018 that China's cyber activity inside the U.S. had risen in recent months. An NSA spokeswoman said that Joyce – a former White House Cyber Adviser to President Trump – was referring to digital attacks against the U.S. energy, financial, healthcare and transportation sectors. Joyce's remarks were notable because U.S. concerns about Chinese hacking had previously centered on espionage and intellectual property theft, rather than attempts to disrupt critical infrastructure.

But it's not just foreign threats you need to be wary of. Your agency must remain ready for external and internal antagonists alike. These foes use everything from botnets to ransomware, and you can't block what you're not expecting. Knowing their motivations and tactics is the difference between success and failure. If you don't take cybersecurity seriously, a strike could cripple your agency's services.

Navigating this hazardous landscape is intimidating, but GovLoop can help you safely make your way. This guide explains today's cyberthreats, what motivates attackers, the damage they can cause and best practices for keeping your organization safe. Key events detailed in this guide will also help you recognize, anticipate and prepare for these enemies.



Foreign Nations

Experts often list China, Iran, North Korea and Russia among the biggest cyber adversaries to the U.S. Each often clashes with American interests, and each also boasts active and aggressive cybersecurity forces.

Foreign governments become antagonistic toward the U.S. for many reasons, including economic competition, religious differences and cultural resentment. Sensitive data about American citizens is a valuable prize for these countries because it can give them an economic, technological and even military edge.

“Foreign actors are the No. 1 threat [to the U.S.],” said William Evanina, Director of the National Counterintelligence and Security Center (NCSC) in the Office of the Director of National Intelligence (ODNI). “We in the government have to do a better job of talking about the damages. We’re losing gigabytes of data. We get OK with nation-states stealing our stuff.”

Speaking at the 2018 Symantec Government Symposium, Evanina said that the FBI estimated that foreign cyberthreats cost the U.S. $5 billion between 2014 and 2015.

One way that agencies can counter these threats, Evanina noted, is by practicing strong asset management. Asset management involves ranking the value of your organization’s resources and shielding them based on importance.

Another strategy is making cybersecurity an agencywide operation by including employees in as many parts of your organization’s cyberdefenses as possible, he added.

Practicing active and aware cyber hygiene can prevent many cybersecurity headaches, he said. For example, being careless about the links you click on is bad cyber hygiene. Mobile technology is another potential gap. Each of the tools Americans use presents a potential entrance for cyberthreats, he said.

Because there are only so many actions that America can take outside its borders, the country will have difficulty stopping governments abroad from becoming cyberthreats, Evanina concluded.

“Part of the defense that we’re trying to enhance is a good offense,” he said. “We have to untie the hands a bit and let our adversaries know we’re in the game.”

KEY EVENT

At the beginning of 2018, Chinese government hackers compromised the computers of a Navy contractor in two breaches, according to a June 2018 Washington Post article. American officials said that the incidents happened in January and February 2018.

The hackers targeted a military organization called the Naval Undersea Warfare Center (NUWC) located in Newport, Rhode Island. The NUWC conducts research and development on submarines and underwater weaponry.

U.S. officials said that the hackers stole 614 gigabytes of highly sensitive data regarding undersea warfare. This trove of information included secret plans to develop by 2020 a supersonic anti-ship missile for use by U.S. submarines.

Dubbed Sea Dragon, the compromised initiative contained details that could harm national security if released, the Navy said. The hackers also took sensor and signal data, submarine radio room information about cryptographic systems, and the Navy submarine development unit's electronic warfare library.

The incident is part of China's longstanding efforts to dull America's military edge. It's also a moment that shows how close foreign powers can get to home.

MAJOR MOMENTS

December 2017

The U.S. attributes the WannaCry 2.0 ransomware attack to North Korea.
Source: ODNI

March 2018

The federal government warns that state-sponsored Russian hackers have repeatedly tried disrupting the cybersecurity of America's electric utility grid since at least 2016.
Source: The Homeland Security Department (DHS) and the FBI

September 2018

The Justice Department (DOJ) charges a North Korean citizen with conspiring to conduct multiple destructive cyberattacks worldwide as part of a hacking group sponsored by Pyeongyang's government.
Source: DOJ

October 2018

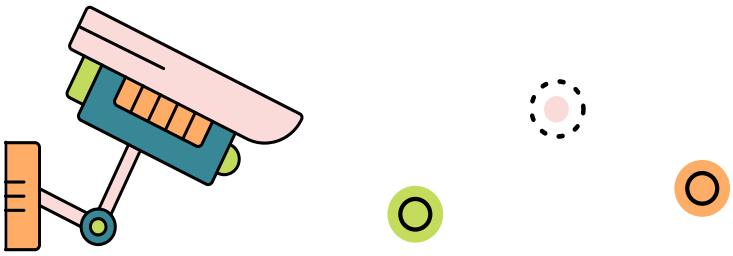
The U.S. charges two Chinese intelligence officers and five hackers they allegedly recruited with trying to steal sensitive commercial aviation and technological data between 2010 and 2015.
Source: DOJ

BEST PRACTICES

1. Rank your resources
based on their importance to your mission, brand and organization.

2. Involve your entire agency in cybersecurity,
including IT, mechanical, procurement, human resources and other departments.

3. Treat sensitive data with the delicacy it deserves
and constantly look for potential cybersecurity risks.



Cyberterrorists

Of all the cyberthreats, cyberterrorism is perhaps the most frightening because it can harm human life.

Cyberterrorists are often motivated by political, religious or social causes, as well as the desire to cause panic. They may act as lone wolves or pledge allegiance to terrorist groups or foreign governments. No matter their affiliation, every cyberterrorist is dangerous.

“This is one of the most sinister and confounding threats in cyberspace,” said Matthew Travis, Deputy Director for DHS’ Cybersecurity and Infrastructure Security Agency (CISA), during the Digital Government Institute’s (DGI) 930Gov Cyber & IT Security Conference 2018. “This is what really keeps us awake at night.”

KEY EVENT

A recent incident illustrates the anxiety cyberterrorists can cause governments and the citizens that they serve.

Multiple U.S. officials confirmed in March 2015 that an online group claiming affiliation with the Islamic State in Iraq and Syria (ISIS) was threatening American military members and their families online.

A group calling itself the Islamic State Hacking Division hacked military databases and posted the names, photographs and addresses of 100 U.S. troops online before calling for supporters to use the information and attack them.

The incident prompted investigations from multiple federal agencies, including the Air Force, Defense Department (DoD), FBI, Marine Corps and Navy. The scare also left many Americans feeling anxious about their safety.

“It is recommended Marines and family members check their online/social footprint, ensuring privacy settings are adjusted to limit the amount of available personal information,” Marine Corps Spokesman Lt. John Caldwell said. “Vigilance and force protection considerations remain a priority for commanders and their personnel worldwide.”

MAJOR MOMENTS

August 2015

A hacker linked to ISIS leaked personal information about 1,300 U.S. military and government personnel in the hopes that they’d be attacked.

Source: DOJ

March 2017

Gen. Joseph L. Votel, Commander of U.S. Central Command (CENTCOM), notes the emergence of a “virtual caliphate” associated with Islamic extremism.

Source: CENTCOM

March 2017

A pro-ISIS media outlet posts a video highlighting potential targets in U.S. cities including Las Vegas, New York and Washington, D.C.

Source: ODNI

December 2017

A screenshot of an ISIS-Somalia video is edited to depict a sniper on a building in Denver, Colorado and then appears online, possibly to inspire extremism or fear.

Source: ODNI

BEST PRACTICES

1.

Exercise caution

about the personal information you put online or share on social media.

2.

Report any suspicious activity

that might involve cyberterrorism to the relevant local, state or federal authorities.

3.

Remember that cyberterrorism thrives on fear,

so stay calm and protect your safety when dealing with potential cyberterrorism incidents.

Cybercriminals

"Cybercrime" is a broad term covering any illegal activity involving cyberspace. For government agencies, however, it's wrongdoing that can inflict real harm.

Many goals motivate cybercriminals, making them difficult to predict and prevent. Some are driven by greed, while others are unhappy with their governments. Other inspirations for cybercrime include religious extremism, political protest and social activism.

Regardless of the cause, however, cybercrime can hurt any agency's resources, reputation and services. For example, hackers targeting a city's 911 centers can halt emergency assistance there.

"There isn't a moment where we can say we're secure in cyberspace," said Jeanette Manfra, Assistant Director for Cybersecurity, DHS CISA, during the ninth annual Billington Cybersecurity Summit. "This is unfortunately not an end state but a continuous journey."

Manfra added that cooperation between the public and private sectors is crucial for defending against dangers such as cybercrime.

"Everybody has a role to play," she said. "We have to be able to share information across these communities so we're not bumping into one another."

KEY EVENT

A hacking incident involving the Securities and Exchange Commission (SEC) shows how costly cybercrime can be for agencies everywhere.

SEC announced in January 2019 that federal authorities had charged nine defendants with hacking a government database holding corporate secrets.

Prosecutors alleged that the hacking occurred in 2016, with the defendants ultimately penetrating the SEC's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system. The hackers stole thousands of documents containing confidential, sensitive information about the financial conditions of multiple corporations. The information was ultimately used to reap at least $4.1 million in illegal trading profits, prosecutors added.

"These threats to our marketplace are significant and ongoing and often involve threats from actors outside our borders," SEC Chairman Jay Clayton said in a statement. "No system can be entirely safe from a cyber intrusion."

A criminal complaint states that the hackers sent SEC employees emails that appeared to come from others inside the agency. Malware infected the targets' computers, which allowed hackers to steal corporate information from the SEC's database.

After the incident, the SEC hired more cybersecurity experts, launched a cybersecurity unit and began an internal review.

MAJOR MOMENTS

September 2014

DOJ charges four alleged members of an international computer hacking ring with stealing Apache helicopter training software from the Army.

Source: DOJ

March 2018

The federal government charges nine Iranian hackers with targeting the Labor Department (DOL), the Federal Energy Regulatory Commission (FERC), and the state governments of Hawaii and Indiana, among other victims, between 2015 and 2018.

Source: DOJ

January 2019

Cybercriminals disrupt public services in Del Rio, Texas while demanding ransom money from the city's government.

Source: Del Rio, Texas city government

January 2019

The city of Akron, Ohio suffers a cyberattack that appears to be "financially-motivated.

Source: Akron, Ohio city government

BEST PRACTICES

1. Recognize that cybercrime covers a broad range of threats

and stay aware of the latest news involving each potential danger.

2. Continuously monitor

your agency's data, personnel, networks and other resources to find, stop and prevent cybercrime.

3. Coordinate with all available public- and private-sector partners

for the latest cybercrime information, resources and tips.

CenturyLink®

The Adaptive Network™

Accelerate network modernization

Secure and reliable network connections are the foundation of IT modernization—but static networks are difficult to maintain and require lots of time, money, and manpower to keep up with ever-changing mission needs.

Analytic-driven networks can ease this burden. They configure, monitor and maintain themselves. Innovative IT leaders are investing in secure, cost-effective, high-performing connectivity to accelerate network modernization in today's hybrid IT and cloud environments.

Ciena's Adaptive Network solutions are available on the Alliant 2 contract, so no matter what your IT modernization strategy demands, CenturyLink and Ciena have your connections.

Contact CenturyLink to see how you can have your network work for you.

Visit us at: centurylink.com/transformingnetworks

ciena

INDUSTRY SPOTLIGHT

How Agile Cybersecurity With Adaptive Networks Can Help Protect Government Agencies

An interview with Jim Westdorp, Chief Technologist, Ciena Government Solutions; and Steve Opferman, Senior Director of Innovation, CenturyLink

Cybersecurity attacks are rising daily in both volume and sophistication. Today, there are more threats to government networks than ever before.

At the same time, government networks are becoming more complex, with newer systems, more sophisticated tools, and innovative technologies being added constantly. If not handled correctly, these new additions can provide more gateways for attackers and diminish network visibility.

Ciena and CenturyLink are combining their technology, years of experience and expertise to help government agencies modernize and secure their networks to meet these challenges head on with Adaptive Networks. In an interview with GovLoop, Jim Westdorp, Chief Technologist at Ciena, and Steve Opferman, Senior Director of Innovation at CenturyLink, explained what an Adaptive Network is and how it can meet organizations' modernization and cybersecurity needs.

Adaptive Networks are automated and programmable networks that can configure, monitor and maintain themselves, as well as adapt to changing requirements. These networks are built on three foundational layers: programmable infrastructure, analytics and intelligence, and software control and automation.

The programmable infrastructure layer acts like a sensor and produces real-time data about network performance and vulnerabilities, allowing agencies to proactively address them and allocate resources accordingly.

The analytics layer, meanwhile, adds intelligence to the network. It applies machine learning to analyze performance data and more accurately predict network problems and threats.

The final layer is software control and automation. It leverages software-defined networking technologies and multi-domain service orchestration to simplify network management and service delivery across multi-vendor, multi-domain hybrid networks.

These layers work together to provide a more intuitive, scalable and secure network.

"The Adaptive Network is putting the functionality and sensors in place for instrumenting the network to determine its state and if there are any problems in it," Ciena's Westdorp said. "Then there's automation and intelligence to analyze the data coming from the network. Finally, orchestration closes the loop and lets you make changes as a result."

The Adaptive Network doesn't sacrifice any fortifications in exchange for the flexibility it gives agencies. Rather, it uses the highest security cryptographic standards available for data transfer. "We can provide ubiquitous encryption across a wide area, and encrypted waves are no longer an impediment in terms of cost or performance," said Westdorp.

An Adaptive Network helps agencies meet rising strains on their bandwidth, as well as modernization and security demands, and deliver high-performance connectivity and faster services to constituents.

"We're leveraging the network as it is today and adding enhancements on top of it," CenturyLink's Opferman said. "It meets agencies' needs in an expeditious fashion without compromising the resiliency that's built into their networks."

"The Adaptive Network meets agencies' needs expeditiously without compromising network resiliency."

– Steve Opferman, Senior Director of Innovation at CenturyLink

MAIN TAKEAWAY

The Adaptive Network is built on three foundational layers – programmable infrastructure, analytics and intelligence, and software control and automation – that work together to provide a more intuitive, scalable and secure network.

Q&A With Rep. Robin Kelly (D-Ill.)

Rep. Robin Kelly (D-Ill.) has focused much of her energy on technology since entering Congress in 2013. Since then, Kelly has made her mark on cybersecurity issues including hacking, workforce recruitment and the Internet of Things (IoT).

For example, Kelly sponsored the House version of the Connected Government Act that Trump signed into law in 2017. The law mandates that updated and redesigned federal websites be mobile-friendly going forward.

Kelly was also a Democratic co-sponsor of the Modernizing Government Technology (MGT) Act, a bipartisan effort that Trump signed into law the same year. The law allows agencies to reprogram their unspent IT budget allocations into working capital funds and use that money for future modernization efforts. The legislation also created the Technology Modernization Fund (TMF), which is a centralized pool of funding that agencies can apply to modernization projects. On becoming law, the MGT Act was celebrated as a major boost to agencies working on IT modernization while responsibly spending their budgets.

Now working in the 116th Congress, Kelly is striving to make IoT cybersecurity a priority for the federal government. IoT devices are any tools that can connect to the internet, presenting a wide range of potential targets for cyberthreats.

Shielding these gaps is critical, and Kelly introduced legislation in December 2018 that would establish cybersecurity standards for all the federal government's purchases of IoT-capable gadgets.

GovLoop spoke with Kelly about various federal cybersecurity topics. In the following Q&A, Kelly discusses IoT regulations, public-private cooperation on cybersecurity and how citizens can practice better cyber hygiene.

This interview was lightly edited for length and clarity.

GOVLOOP: What does the federal government do well in terms of cybersecurity and where is it struggling?

KELLY: On cybersecurity, we have a good idea of what we need to do. There are clear lists of needed steps to enhance cybersecurity, but the challenge remains funding and the required empowerment of CIOs and others to take the necessary steps to improve cybersecurity. We are making progress. We are a lot better than we were two years ago, but we still have a lot of work.

GOVLOOP: What cybersecurity challenges are unique to the House and congressional representatives?

KELLY: The cybersecurity challenges for congressional offices are twofold. First, each office and its procurement are handled independently. Secondly, offices have a Washington, D.C. location as well as one or more district locations.

In recent years, cybersecurity training has been mandated and expanded for staff, and this has helped address some of these vulnerabilities.

GOVLOOP: How would you rate the Trump administration's efforts on federal cybersecurity? Why?

KELLY: The administration's efforts on federal cybersecurity have been hit and miss. On an executive branch policy level, the administration has taken some disappointing steps. *(GovLoop: Kelly has previously criticized the Trump administration's handling of Russian cyberattacks, for example, and congressional Republicans' steps to protect cybersecurity during the 2018 midterm elections.)*

At the agency level, we are starting to see real progress on IT modernization and cybersecurity enhancement. This has largely been driven by the congressional accountability created by the FITARA scorecard. *(GovLoop: FITARA refers to the Federal Information Technology Acquisition Reform Act. The legislation gave agency CIOs stronger powers for helping their organizations modernize IT. The House Oversight and Government Reform Committee now issues biannual scorecards to grade agencies on how well they comply with FITARA's IT modernization requirements.)*

GOVLOOP: How would you describe IoT to constituents who aren't familiar with it?

KELLY: IoT is everything – other than a computer or cellphone – that can connect to the internet. Your webcam, Fitbit or even your "smart" refrigerator is each an IoT device.

GOVLOOP: Your recent House bill would set various federal standards for IoT cybersecurity for the first time. What standards do you believe are the most useful for defending U.S. cybersecurity?

KELLY: If IoT devices are going to be used in coordination with devices attached to government networks, we need to be 100 percent sure that these IoT devices are not creating a backdoor for hackers and cybercriminals to access government networks and data.

My IoT bill is a basic cybersecurity hygiene effort to protect our networks and the sensitive data of American families. My legislation empowers the experts at NIST [the National Institute of Standards and Technology] to populate these standards while allowing agency-level flexibility as new technological innovations create other IoT devices that should assist in delivering government services.

GOVLOOP: What role – if any – do you think the federal government should have in regulating the private sector in terms of cybersecurity?

KELLY: The federal government should set the floor for cybersecurity standards. The industry has shown leadership in innovating cybersecurity solutions, and the government can and should engage industry to advance best practices.

GOVLOOP: What best practices would you recommend to citizens for protecting their own cybersecurity, including in terms of IoT devices?

KELLY: Understand what you bought and know that cheaper isn't always better. Unfortunately, there are a lot of manufacturers who leave backdoors or take shortcuts that endanger a person's cybersecurity. There are a good number of sites and industry-based certifications that can help inform consumers.


FORTINET
BE READY.
Fortinet has the only NSS Labs "Recommended" SD-WAN solution with security
Learn more at ready.fortinet.com

INDUSTRY SPOTLIGHT

Modernizing Your Network Security With SD-WAN

An interview with Nirav Shah, Senior Director, Product Marketing, Fortinet and Felipe Fernandez, Director, Systems Engineering, Fortinet Federal

The race is on to modernize agencies' IT networks so that they can deliver better public services and reduce costs.

Unfortunately, security sometimes trails the threats endangering these networks. Federal, state and local organizations are finding themselves exposed to dangers such as cybercriminals and insider threats when their networks grow faster than they can modernize them.

To understand how agencies can modernize their networks while enhancing security, GovLoop spoke with Nirav Shah, Senior Director of Product Management at Fortinet, and Felipe Fernandez, Director of Systems Engineering at Fortinet Federal. Fortinet is a cybersecurity hardware, software and services provider that delivers secure software-defined wide area networks (SD-WANs).

SD-WANs simplify the management and operations of computing and telecommunications edge networks. The technology differs from traditional wide area networks (WANs) by separating the networking hardware and the mechanism for controlling it across the vast physical space between them. It's a division that strengthens network security without degrading services or increasing costs.

Fernandez said that agencies have long struggled with contracting fair priced, reliable internet services across their networks. "Not all agencies' sites are in prime internet hubs," he said. "Some are in remote locations that have limited options for a WAN."

Geographical considerations have often made networks too complex for agencies to handle easily, Shah added. SD-WANs solve this dilemma by streamlining IT networking management.

"SD-WANs are top-of-line because they have changed how agencies can adopt applications and use them more efficiently," he said. "SD-WAN is a technology that simplifies your business operations. You're doing that at a lower cost with better security."

Shah said that SD-WANs are additionally valuable as they ensure agencies have consistently reliable networks for business operations.

"Our SD-WAN is built to transform your entire office," he said. "It's all part of that major goal of simplicity, better productivity and consistent security."

Security, however, becomes increasingly difficult as organizations try aligning modern technologies with government security standards, some of which don't reflect new business methods. Federal agencies, for example, must follow the Office of Management and Budget's (OMB) Trusted Internet Connection (TIC) program. TIC strives to reduce the number of the federal government's external network connections. In December 2018, OMB released a draft update to TIC that lists cloud models that comply with the program's security standards.

Fernandez said that SD-WANs help agencies improve network performance as well as comply with TIC and other benchmarks, such as the National Institute of Standards and Technology's (NIST) cybersecurity framework.

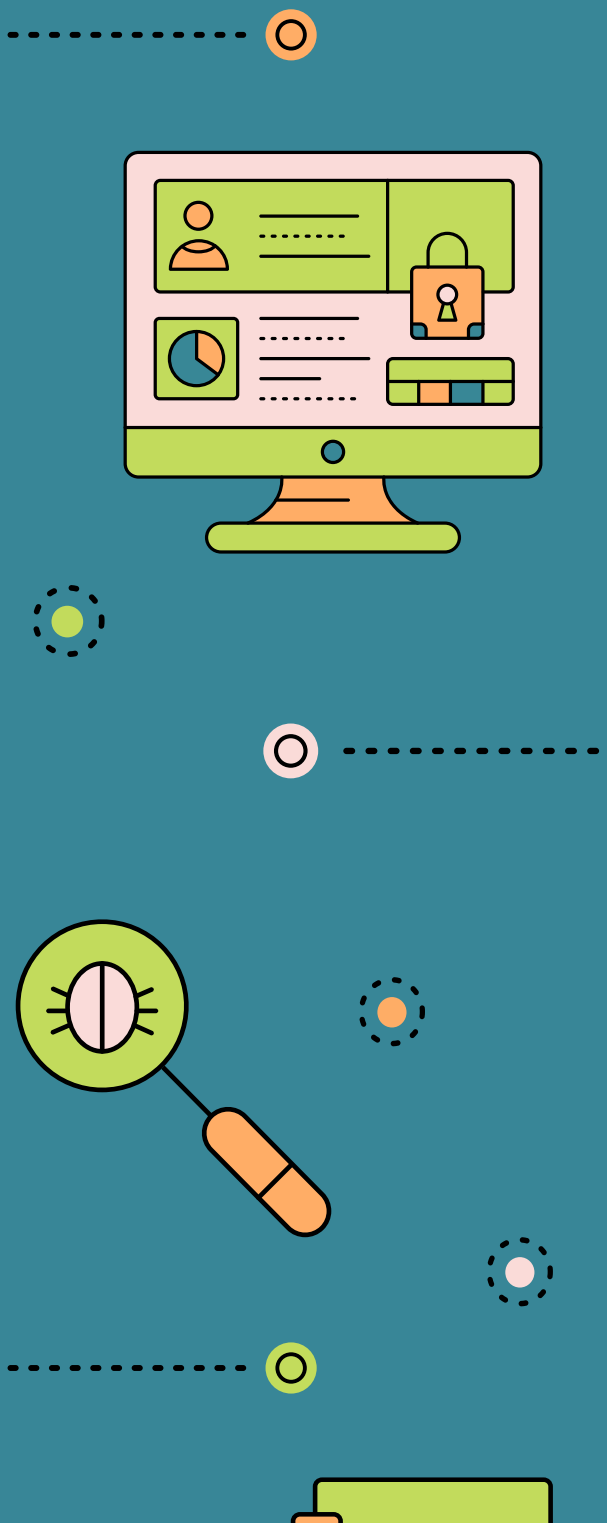
These best practices and guidelines for federal security often inspire similar behavior from state and local governments. SD-WANs help all organizations by providing secure, highly available networks for every size agency.

"SD-WAN is built to transform your entire office. It's all part of that major goal of simplicity, better productivity and consistent security."

– Nirav Shah, Senior Director, Product Marketing at Fortinet

MAIN TAKEAWAY

SD-WANs modernize agencies' networks while enhancing security, simplicity and access to reliable services across geographical distances.



Ransomware

Ransomware is a troubling tactic increasingly used against agencies. It's malicious software that freezes computers and computer-controlled equipment until the victim pays a ransom to the executor.

All agencies are vulnerable to ransomware. At best, it disrupts public services until they can resolve an attack. At worst, it interrupts government functions while forcing agencies to pay their attackers.

Cybercriminals use ransomware to turn a profit, but it's also quickly becoming a weapon that foreign governments, cyberterrorists and other antagonists use. That's particularly dangerous because it may affect national security or public safety.

Regardless of the attacker, ransomware is a growing menace to agencies that the public is just starting to understand.

KEY EVENT

Atlanta is an example of the chilling effect that ransomware can have on governments anywhere, regardless of their size.

According to DOJ, two Iranian nationals executed a ransomware attack against Atlanta's city government on or about March 10, 2018, that lasted about 12 days. The attack impaired major government services and caused millions of dollars in losses.

The ransomware, known as "SamSam," used in the attack infected roughly 3,789 computers, including servers and workstations, belonging to Atlanta's city government, DOJ said.

Once deployed, the ransomware encrypted the files associated with each infected computer before displaying a ransom note. Information on the infected machines was effectively locked until the ransom was paid and users received a decryption key.

In December 2018, a federal grand jury indicted Faramarz Shahi Savandi and Mohammed Mehdi Shah Mansouri for the incident, DOJ said in December 2018.

The indictment – filed in the U.S. District Court for the Northern District of Georgia – charged both men with intentional damage to protected computers located in Atlanta that caused losses exceeding $5,000.

The charges also allege that the pair affected more than 10 protected computers and threatened public health and safety.

Kimberly A. Cheatle, Special Agent in Charge of the Secret Service's Atlanta Field Office, said that the incident is a teachable moment for agencies nationwide.

"This case serves as a reminder, particularly during the holiday season, to ensure protocols related to cyber hygiene are observed," she said in December 2018. "The Secret Service appreciates the level of cooperation and information sharing throughout this investigation by all law enforcement partners which led to this indictment."

The latest Census Bureau (USCB) data available at the time of the attack shows the impact that such incidents can have on citizens. Atlanta had an estimated population of about 486,000 people before the incident, meaning all those people may have lost the public services their tax dollars pay for during the ransomware holdup.

MAJOR MOMENTS

December 2017

Multiple public services are frozen when a ransomware attack strikes Mecklenburg County, North Carolina.
Source: Mecklenburg County, North Carolina government

February 2018

The Colorado Department of Transportation (CDOT) is attacked with ransomware.
Source: GovLoop

September 2018

A cyberattack disrupts the port of San Diego, California's IT systems, disrupting multiple public services
Source: The port of San Diego, California

October 2018

A ransomware attack disables several city servers in Muscatine, Iowa.
Source: Muscatine, Iowa's city government

BEST PRACTICES

1.

Isolate computers, networks or systems infected by ransomware immediately

so that the problem does not spread throughout your agency.

2.

Have a business continuity plan in place

for ransomware attacks to prevent disruptions in public services and internal operations.

3.

Do not pay the ransom

as there's no guarantee you will regain access to your agency's impacted data.

Insider Threats

All the external defenses in the world can't stop a threat that comes from within. This harsh reality means that insider threats are one of the most potentially damaging menaces facing governments.

The U.S. Computer Emergency Readiness Team (US-CERT) defines insider threats as any "current or former employee, contractor, or other business partner who has or had access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity or availability of the organization's information or information systems."

Insider threats can come in the form of fraud, computer infrastructure sabotage or theft of confidential or commercially viable information. Even worse, insider threats are difficult to detect as they lurk inside an agency rather than breach it from the outside.

Stopping insider threats is difficult because any individual with access to an organization's internal information is a risk. That means they can inflict harm accidentally or intentionally. Furthermore, an agency's business associates and contractors can also become insider threats if they mishandle sensitive information.

Recognizing the danger from insider threats, former President Barack Obama issued Executive Order 13587 in 2011 to combat them in the federal government. The executive order tasked the heads of all federal agencies accessing or operating classified computer networks with implementing an insider threat detection and prevention program. The directive also established the National Insider Threat Task Force (NITTF) for fighting the problem governmentwide.

Though well-intentioned, Obama's order has not stopped federal insider threats completely. A 2018 GovLoop survey of 170 federal employees found that 46 percent say insider threats are a rising challenge at their agency. The executive order also didn't help state and local governments that are as vulnerable to insider threats as federal agencies.

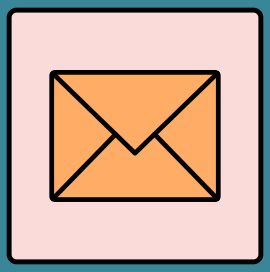
So how can agencies prevent insider threats? One solution is vetting the trustworthiness of your organization's technology staff.

"Every day in the newspapers there's a new story about a person who became an insider threat at an agency," Evanina, ODNI's NCSC Director, said at the 2018 Symantec Government Symposium. "They're a dime a dozen. You need to know who you're hiring in your IT shop or CIO shop. Are they trusted?"

Another option is recognizing that strong cyber hygiene is an ongoing effort. Agencies that become lax about their cybersecurity are more likely to create accidental insider threats, whereas organizations that continuously train workers about detecting cyberthreats and keeping their data safe reduce their risk.

"You'll never solve cyber hygiene problems," NSA Program Director Cheri Caddy said at the symposium. "It will continue to be a consistent problem."

Emerging technologies are a third counter to insider threats. Tools such as automation, machine learning and artificial intelligence (AI) are helping humans find, stop and prevent insider threats by spotting unusual behavior, information access and log data. Organizations can also use these tools to find external cyberthreats that are targeting privileged users who interact with sensitive insider information.



KEY EVENT

Minnesota's Department of Public Safety (DPS) is proof that people with access to sensitive data can become insider threats and cause major headaches for their governments.

DPS confirmed in January 2019 that the agency wrongfully turned over personal information on scores of citizens to three private companies in late 2018.

Spokesman Bruce Gordon said that DPS "inadvertently" sent the addresses of 1,500 people who had registered their vehicles with Minnesota's state government to Experian, Polk and Safety First during the incident. Affected citizens had asked that their information remain private once they registered their vehicles – a request that was ultimately not fulfilled.

"There was no data breach," Gordon said, noting that there is no indication "that private data has been accessed or used unlawfully."

He added that Minnesota's government notified all the vehicle owners affected by the incident, and the state's IT services changed DPS's bulk motor vehicle file to remove the records concerning people who had requested that their personal information remain private.

"Making sure that certain data are private is a responsibility we take very seriously," he said.

Minnesota Legislative Auditor Jim Nobles, meanwhile, said in January 2019 that DPS failed to provide him with information about the breach, forcing him to use his subpoena powers for the first time in his 35-year career.

"It's my understanding – in fact, it's my knowledge – that the department has in fact informed individuals that their data was inappropriately sent to certain companies," he said in Minneapolis.

Nobles added that he is unsure how many citizens had their information compromised during the event. "That is something we are still looking at," he said.

DPS's data situation is a cautionary tale for agencies about carefully governing who can access their sensitive data and how that information is handled.

Agencies that fail to stop insider threats risk having their finances, reputations and services damaged by cybersecurity incidents.

MAJOR MOMENTS

November 2015

Brian Kemp, then Georgia's secretary of state, acknowledges that his office had illegally disclosed the Social Security numbers of more than 6 million registered voters due to a "clerical error."

Source: Georgia Secretary of State's office

June 2017

Reality Winner, then an NSA contractor, is charged with removing classified material from a government facility and mailing it to a news outlet.

Source: DOJ

February 2018

The California Department of Fish and Wildlife (CDFW) discloses a data breach involving a former state employee that was discovered earlier in the year.

Source: CDFW

September 2018

Nghia Hoang Pho, a former NSA developer, is sentenced to 66 months in prison for removing and retaining U.S. government property – including top-secret national defense information – between 2010 and 2015.

Source: DOJ

BEST PRACTICES

1. Practice consistently strong cyber hygiene

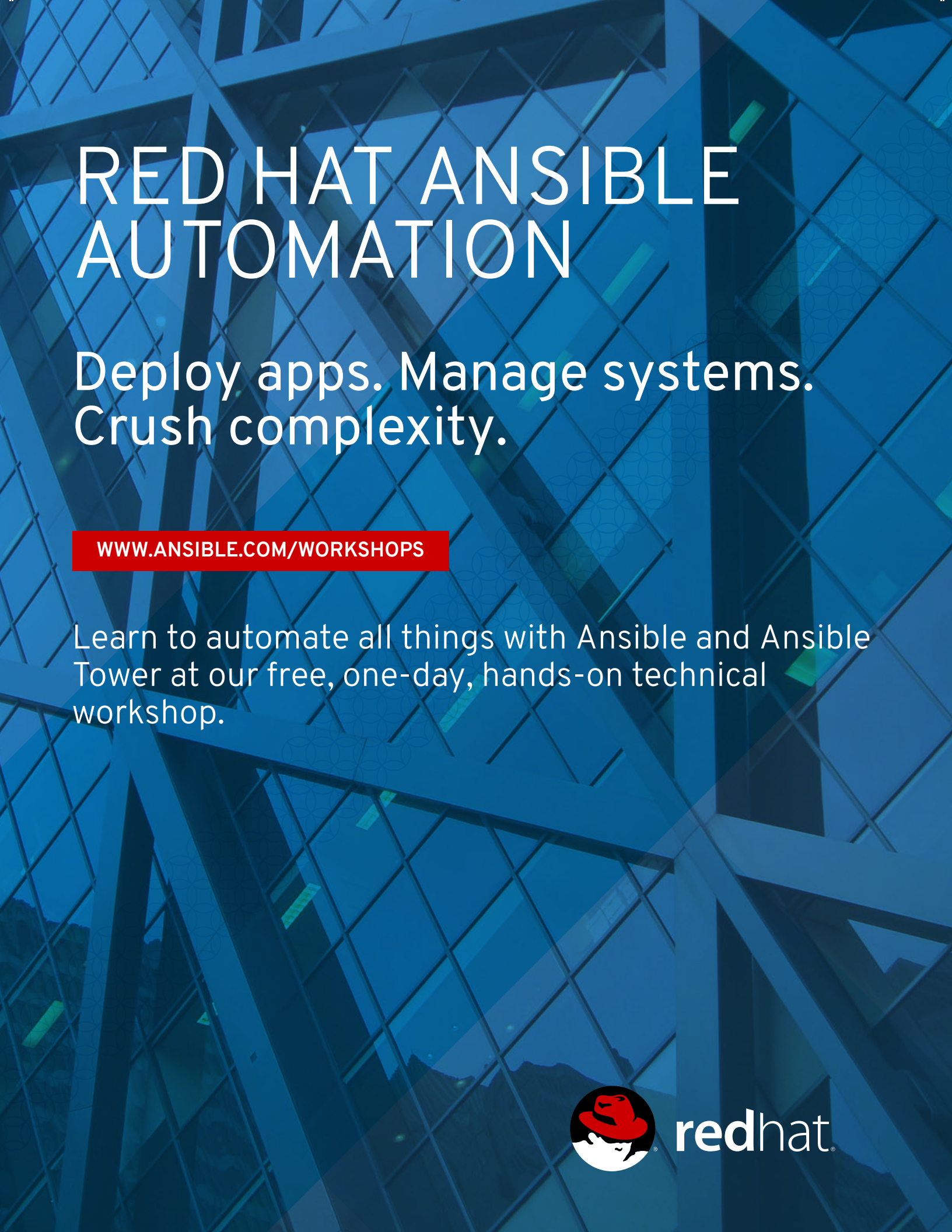
to reduce the risk of an accidental insider threat at your agency.

2. Monitor problematic or departing staff

for the potential to become either accidental or intentional insider threats.

3. Tightly govern access

to sensitive data so that people are not potentially mishandling agency information.


RED HAT ANSIBLE AUTOMATION
Deploy apps. Manage systems. Crush complexity.
WWW.ANSIBLE.COM/WORKSHOPS
Learn to automate all things with Ansible and Ansible Tower at our free, one-day, hands-on technical workshop.
redhat.

INDUSTRY SPOTLIGHT

Automating Your Security at the Edge

An interview with Chris Reynolds, Senior Cloud Architect, Red Hat

Government networks extend farther than ever, and the number of devices that can connect to these networks is growing. Although this gives employees greater connectivity, more devices also mean more challenges for agencies and the citizen data that their workforces handle.

Thankfully, automation can keep federal, state and local organizations from exposing themselves to unforeseen cybersecurity risks. Automation speeds up service delivery while reducing human error, helping government employees protect sensitive information while completing their missions.

To understand how agencies can automate security at the network edge, GovLoop spoke with Chris Reynolds, Senior Cloud Architect at Red Hat, an open source software solutions provider.

According to Reynolds, cybersecurity is an agencywide effort that will increasingly need automation as agencies embrace the Internet of Things (IoT). IoT networks include sensors and devices that can collect, store and exchange data via the internet.

"Something as simple as automating the ability to change default usernames and passwords on IoT devices can improve the security posture of agencies that are using those devices," he said.

Reynolds noted that IoT tools are often attractive to cyberthreats because of their data handling. IoT devices process data before sending the information to a cloud or data center. This data is vulnerable when agencies don't change the default credentials on their IoT devices quickly enough.

Automation can also immediately patch gaps that emerge in agency operating systems, Reynolds continued. Patching becomes an automated, recurring activity that frees up system administrators to focus elsewhere within their agency's infrastructure.

As their network infrastructure grows, more agencies are adopting hybrid cloud. Hybrid cloud combines public and private clouds, letting agencies choose the cloud environment that is most appropriate to host their data depending on its sensitivity level.

Reynolds added that automation is also useful for managing application programming interfaces (APIs). APIs are the building blocks for software and other computing tools. According to Reynolds, APIs are crucial for supporting hybrid clouds. Agencies with common APIs between their cloud and on-premise data centers can grow and scale quicker.

Reynolds argued that automation is vital for building hyperconverged infrastructures (HCIs) and cloudlets. HCIs are IT infrastructures where software virtualizes all the system's hardware-defined components. Cloudlets, meanwhile, are mobile cloud datacenters. HCIs, cloudlets and the APIs supporting them are all major cybersecurity concerns due to the data they handle.

"HCIs consolidate compute, storage and networking into a manageable framework, allowing agencies to reduce their manpower and overhead," he said. "Cloudlets bring the cloud closer to mobile devices, helping complete massive computational work in the field before sending the results back."

Reynolds concluded that open source software and automation are a powerful cybersecurity pairing. "Agencies can scale, secure, react and respond to anything they encounter with open source software solutions such as Red Hat's," he stated.

"Something as simple as automating the ability to change the default usernames and passwords on IoT devices can improve the security posture of agencies that are using those devices."

– Chris Reynolds, Senior Cloud Architect at Red Hat

MAIN TAKEAWAY

Automation helps ensure strong cybersecurity for agencies' networks, IoT devices, hybrid clouds, HCIs, cloudlets and more.

State CIOs Discuss Cybersecurity

In some ways, cybersecurity is a greater risk to state agencies than their federal counterparts. State governments often have smaller budgets and workforces than federal organizations, meaning they have less resources for handling the same cyberthreats.

As a result, adversaries may even view states as easier, more appealing victims as their governments' assets are more constrained. It's a recipe for disaster in an era of frugal funding and difficult cybersecurity talent recruiting.

GovLoop recently spoke with Colorado's and Mississippi's CIOs about their cybersecurity journeys. The following insights shed light on cyber hygiene, ransomware, defending against cyberattacks and more.

The responses below were lightly edited for length and clarity. These excerpts focus on cybersecurity and were taken from full interviews conducted as part of GovLoop's recurring "CIO Conversations" series.

Mississippi CIO Craig Orgeron

GOVLOOP: What are some recent developments in Mississippi's cybersecurity landscape?

ORGERON: In 2017, Mississippi's legislature provided great leadership in passing House Bill 999, which enacted the first-ever enterprise security statute for Mississippi. It put in statute the roles and responsibilities of Mississippi's Information Technology Services Department [ITS], the roles and responsibilities of agencies, and it formally enabled a security template – literally a collaborative body that was going to approach security questions in the state collectively.

We had a program before 2017, but that was a big move. We remain focused on the culture of cyber in advocating for training, basic hygiene and awareness in agencies, and we have other projects.

GOVLOOP: What cyber challenges are you facing?

ORGERON: We haven't necessarily seen an uptick in ransomware that would be catastrophic. Some of the bigger issues are cyber culture and hygiene. That's a challenge because of the weakest-link mentality.

Cyber is like insurance or going to the dentist. You could possibly get by without going to the dentist for four or five years. Hey, you brush your teeth, and you're good. But when you get the cavity, you kind of regret not going.

In some ways, cyber can be somewhat thankless because you can rock along for a while, regardless of what's happening under the hood, and maybe not run into a problem. And I think that's the most toxic potential message, right? Nothing bad has happened, therefore...I think there's a constant challenge to stay vigilant.

Colorado CIO Theresa Szczurek

GOVLOOP: What are Colorado's biggest cybersecurity concerns, and how are they impacting how you address citizens' needs?

SZCZUREK: Cybersecurity is on everybody's mind and is a top priority to keep our state systems secure. We have a chief information security officer [CISO] and a staff that is working to ensure that the 8.4 million security events the state of Colorado gets per day are deflected.

We have a whole program that is working constantly to respond to this while also being very proactive. We have something called the Backup Colorado initiative, which we used last year during a cyber crisis. Because of the platform we have in place, we were able to recover up to 80 percent of data within just four weeks. No data was lost, and no ransom was paid.

We take this very seriously. We're inserting two-factor authentication as an added extra layer of security. We are educating state employees. Believe it or not, one of the biggest risks when it comes to cybersecurity is employee negligence and bad habits. We have quarterly cybersecurity trainings to promote good cyber habits, like just putting your machine into sleep mode when you're not at your desk.

GOVLOOP: What impact does cybersecurity have on Colorado's workforce in terms of cyber hygiene, training and recruitment?

SZCZUREK: Colorado is respected nationally for our cybersecurity work. We have been going around the state, to NASCIO [the National Association of State Chief Information Officers] and other organizations, and then we were invited to share what we've learned. This is attracting people who are talented to think, "Wow, if I'm going to pursue a career in cybersecurity, I want to consider working for the state of Colorado."

We're also educating the next generation of college students. We have a whole group of them onsite today, and we're teaching them about the importance of careers in cybersecurity and how this is a job that gives you great security in the sense that you're always going to be in demand.

We're always looking at our policies, we're training our people and we're going into the broader community. Our employee performance plans, for example, include cybersecurity training requirements because it's important that everyone understands how they can take little and big steps to protect this most critical resource.

There are also not only the computers and hardware, but there are the databases and all the data too. We have a chief data officer in our organization who is looking at the data that we have. Some of it is posted publicly on a website that people can get access to because this is an asset of the people of Colorado. It is our responsibility to protect it. Now, there's certain proprietary information like HIPAA [the Health Insurance Portability and Accountability Act of 1996] and personal information that is not public, but we're also protecting that so that you don't get a disaster like any of the increasing number of companies that have been attacked recently.

GOVLOOP: What are some best practices in cybersecurity that you'd recommend to other government officials?

SZCZUREK: I think you should have the 20 Center for Internet Security (CIS) controls in place and then figure out what programs are best to implement considering the individual needs of your government. We have programs in place that protect our inventory of equipment both actively and passively, and we're doing continuous vulnerability management so that we rate the risk of certain vulnerabilities, and then we prioritize them based on their potential impact for remediation. We have certain scanning tools that allow us to keep our pulse on what's happening.

At a very practical level for our employees, we have a policy protecting them from phishing. We say, "Don't click. If you receive an email that's suspicious, just delete it. Do not click on anything in the email. You know some emails are created to grab information or install malware, regardless of where you click in the email." Some scams even come by phone call. We make our employees aware that if you receive a suspicious phone call, hang up immediately. You would be surprised to know the information that an attacker could gain through something like that.

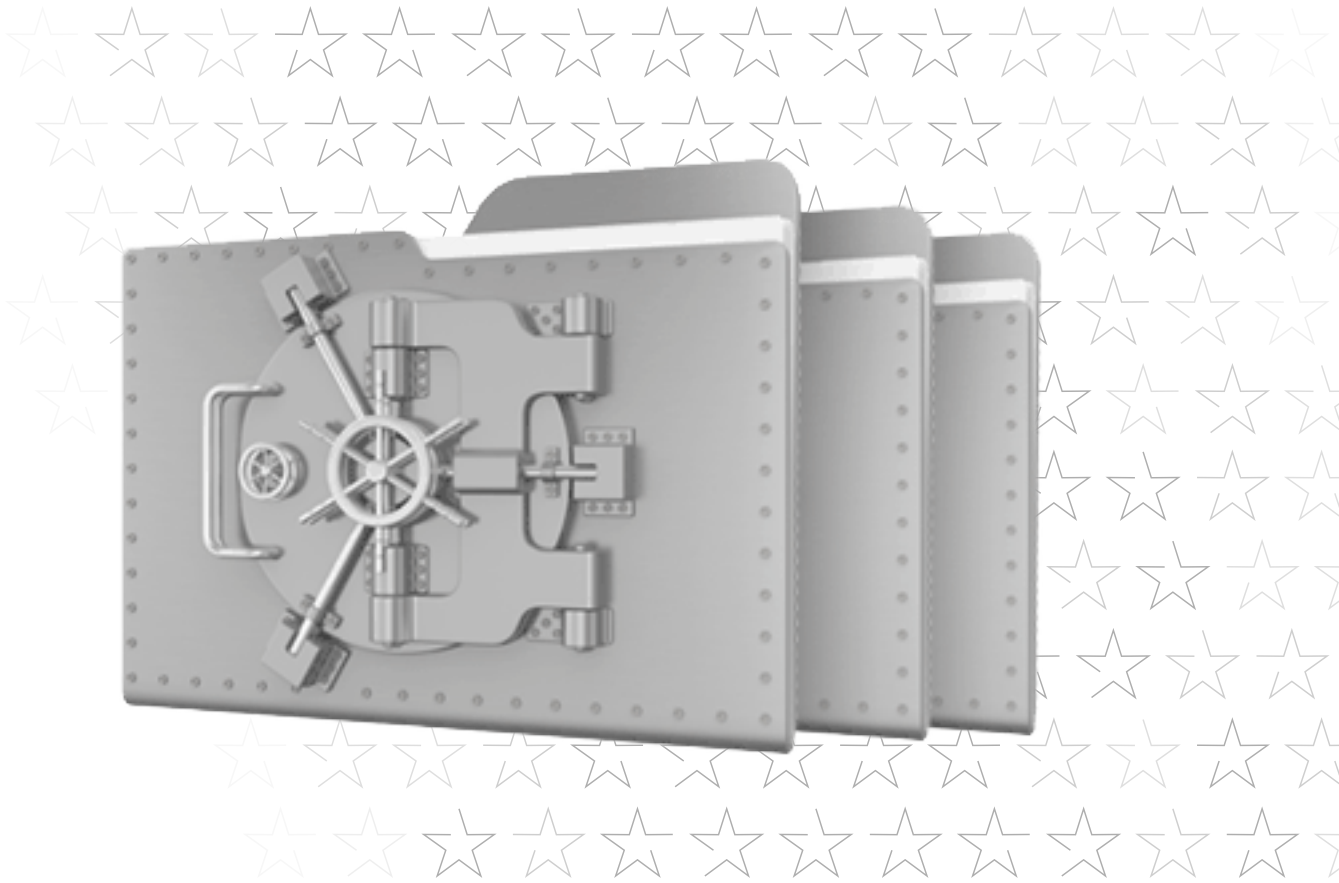
We use extreme caution when connecting a USB drive to a state computer. Malware and viruses are often transferred easily through USB drives. We're also very careful about what software is added to our state computers, and we have a whole approach. We want people to just think about security in everything they do. A minor mistake can have far-reaching security impacts.

solarwinds government

Security just got real.

Powerful. Affordable. Easy to use.

Scalable, end-to-end IT monitoring software
from solarwinds.com/government



ACCESS RIGHTS MANAGEMENT

THREAT DETECTION

SECURITY INFORMATION & EVENT MANAGEMENT

PATCH MANAGEMENT

CONFIGURATION MANAGEMENT

MANAGED FILE TRANSFER

FTP SERVER

SOLARWINDS FEDERAL DISTRIBUTOR DLT

INDUSTRY SPOTLIGHT

Improving Your Security Posture to Protect Against Any Threat

An interview with Mav Turner, VP of Product Strategy, SolarWinds

Agencies at every level are facing a growing number of diverse cyberthreats. According to SolarWinds' 2019 Federal Cybersecurity Survey, 56 percent of federal government IT leaders consider careless or untrained insiders the most significant threat to their organizations. Fifty-two percent, meanwhile, said that foreign governments are the primary menace to their agencies.

To learn how agencies can best defend themselves against cyberthreats, GovLoop sat down with Mav Turner, VP of Product Strategy at SolarWinds. SolarWinds works with DLT, a government solutions aggregator, to offer IT management and monitoring solutions for government networks, applications, cybersecurity and more.

"The foreign government risk has continued to rise substantially over the five years since SolarWinds began conducting this survey," Turner said. "Insiders continue to be a threat from a malicious perspective, but they're also something foreign governments can leverage to have a successful attack."

Foreign governments target American agencies for reasons including economic and military competition. Insider threats, meanwhile, are anyone with access to an organization's internal assets.

Turner said that insider threats are especially hard to predict as they can be permanent employees, contractors or temporary employees. Insider threats can also act accidentally or intentionally, making them even more confusing.

"To minimize the risk from insider threats, ensure that employees can only access systems within the scope of their responsibilities," he said.

The survey wasn't all doom and gloom. In fact, respondents noted three areas that are helping them better manage their cybersecurity risks: government mandates, employee training programs and IT security tools.

Turner noted that cybersecurity mandates – such as the Federal Information Security Management Act (FISMA) – help agencies improve their security posture by providing practical best practices and allowing agencies to prioritize how to have the biggest impact on their mission.

Training was another area that respondents noted. "Training isn't just onetime employee onboarding training," Turner said. "It's also quarterly and annual trainings that are tailored to specific job roles and educate employees on how to identify and respond to a variety of attacks."

The final area that helped respondents detect and prevent attacks was IT security tools. Turner recommends that agencies combine patch management, security information and event management (SIEM) and access rights management tools to ward off cyberthreats. Patch management tools ensure that agencies' can address software vulnerabilities without spending a lot of time applying and tracking patches manually. Access rights management, meanwhile, monitors user access permissions and access rights to files and systems to prevent data loss and security breaches. SIEM tools, finally, make it easier to use event logs to detect suspicious activity and demonstrate mandate compliance.

"The key thing is knowing what data you are collecting, who has access to it and ensuring it's secure," Turner said. "SolarWinds brings these tools together so you have a holistic view of your security posture and can quickly detect and respond to threats."

"The key thing is knowing what data you are collecting, who has access to it and ensuring it's secure."

– Mav Turner, VP of Product Strategy, SolarWinds

MAIN TAKEAWAY

The danger from cybersecurity threats such as foreign governments and insider threats is growing, but government mandates, employee training, IT security tools and best practices can help agencies manage these risks.

Hacktivists

Hacktivism is the use of hacking and other cybersecurity tools for promoting a political or social agenda. The wide range of issues that inspire hacktivists means that every agency has reason for concern about them.

Hacktivists are either tech-savvy loners or associate with online groups such as Anonymous, a global, decentralized group whose members often engage in hacktivism. Either way, they're a potentially painful nuisance for federal, state and local organizations. These cyberthreats can interrupt public services, and the cost of the additional government employees and technology needed to stop them can trickle down to taxpayers.

Predicting what hacktivists will do – and when – is additionally challenging. They might dislike government generally or a specific event, law or policy might spur them to act.

KEY EVENT

Baltimore's city government is a testament to how hacktivists can strike when your agency's most vulnerable to make their point known.

Documents that are now publicly available state that the city government's website was crippled in May 2015 during a separate, physical crisis there that started in April.

At the time, Baltimore was under curfew following riots over the death of Freddy Gray in April 2015. Gray, a 25-year-old black man, died one week after suffering a severe spinal injury while in city police custody.

Hackers outraged by Gray's death chose that moment to hit the city government's website, shutting it down for at least 16 hours in May 2015.

According to the documents, someone claiming allegiance to Anonymous posted a message online on April 25, 2015, addressing Gray's death, urging more protesters to appear on Baltimore's streets and demanding that Anonymous members hack the city's websites to publicly release information about the incident.

Meanwhile, other Baltimore city documents also detail attempts at the time to leak information about specific police officers.

Such actions make a bad situation worse by disrupting public services, exposing sensitive data or disrupting your organization's presence online.

MAJOR MOMENTS

December 2014

A hacker launches a cyberattack against the St. Louis County Police Association website over the fatal police shooting of an unarmed black man in Ferguson, Missouri.

Source: DOJ

May 2016

Anonymous tries hacking North Carolina's government over a state law requiring people to use the bathroom corresponding to their biological sex at birth.

Source: North Carolina Department of Information Technology (DIT)

June 2017

All 11 Ohio state government websites are defaced with pro-ISIS, anti-Trump messages.

Source: Ohio Department of Administrative Services (DAS)

May 2018

Hackers upset with proposed legislation to make unauthorized computer access illegal in Georgia target websites in protest.

Source: Electronic Frontier Foundation (EFF)

BEST PRACTICES

1. Rank your resources

based on their importance to your mission, brand and organization.

2. Involve your entire agency in cybersecurity,

including IT, mechanical, procurement, human resources and other departments.

3. Treat sensitive data with the delicacy it deserves

and constantly look for potential cybersecurity risks.

The Future of Cybersecurity

Cybersecurity is an endless battle, and everyone involved in fighting it is always looking for a new edge over their opponents. Subsequently, innovation is constantly changing both cyberthreats and cyberdefenses.

For example, the amount of cyberthreats will grow in proportion to the number of new technologies that become widely used. Technologies that present potential problem areas in the future include autonomous vehicles, drones and IoT devices.

Many emerging technologies, meanwhile, show great promise as potential cyberdefenses. AI may reduce the burden on humans by aiding their cyberdefenses. Blockchain, for its part, is earning accolades for the possibilities surrounding its secure data storage.

Other methods for protecting against cyberthreats are well-established. Practicing smart cyber hygiene will always keep organizations safe, as will complying with all relevant cybersecurity regulations.

Agencies have made significant strides on cybersecurity since federal, state and local governments began using data and IT systems. Despite this, there's always room for improvement on cybersecurity.

KEY EVENT

IoT is the network of internet-connected devices. As more gadgets become IoT-capable, more become potential cybersecurity risks too.

Recognizing the potential for IoT cyber vulnerabilities, Rep. Robin Kelly (D-Ill.) introduced House legislation in December 2018 aimed at strengthening the technology's cyberdefenses.

"As the government continues to purchase and use more and more internet-connected devices, we must ensure that these devices are secure," she said in a statement. "Everything from our national security to the personal information of American citizens could be vulnerable because of security holes in those devices."

Kelly's legislation would require basic cybersecurity standards to be included in all government-purchased IoT devices. For example, the bill would require the federal government to only buy IoT tools that accept security patches and allow users to change their passwords.

"It's estimated that by 2020 there will be 30 million internet-connected devices in use," Kelly said. "As these devices positively revolutionize communication, we cannot allow them to become a backdoor to hackers or tools for cyberattacks."

Under Kelly's legislation, vendors would also be required to notify agencies of any security vulnerabilities they discover, and issue software updates as new dangers emerge.

Kelly's bill would additionally task DHS and the Office of Management and Budget's (OMB) leaders with making a database of noncompliant IoT devices. The agencies would have 180 days to make the database, which would also list IoT tools that no longer receive security updates.

Lawmakers have long shielded citizens by regulating industries, and Kelly's bill suggests that IoT is no exception. Legislation is one tactic governments everywhere can use to establish better cybersecurity practices now and avoid major problems later.

MAJOR MOMENTS

July 2018

DHS launches the National Risk Management Center (NRMC) to protect critical U.S. infrastructure including federal cyber networks.

Source: GovLoop

September 2018

California becomes the first state with laws mandating basic security standards for IoT devices.

Source: GovLoop

October 2018

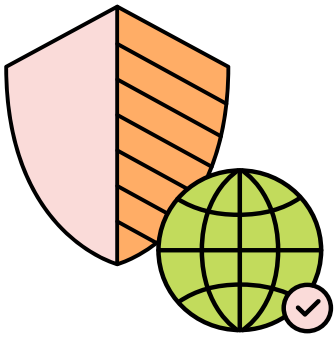
DHS announces that adoption of the strongest level of email authentication enforcement standards had increased by eight times across the federal government in one year.

Source: DHS

November 2018

Cybersecurity and Infrastructure Security Agency (CISA) starts, expanding DHS's mission to include protecting civilian cybersecurity.

Source: CISA



Conclusion

Agencies can't defend themselves against enemies they don't understand. For governments, recognizing the threats surrounding them is vital for keeping citizen data safe.

Cyberthreats don't follow a schedule, however, and stopping them requires constant vigilance. Agencies that let their guard down risk embarrassing cybersecurity incidents that drain their resources and the public's goodwill.

Strong cybersecurity is also easier said than done, and today's agencies need knowledgeable workforces equipped with the best cyberdefenses. Though cyberthreats will always remain dangerous, technology and people can overcome them by working together.

Most importantly, cybersecurity has real-world implications regardless of the type of government involved. Successful cyberattacks can spread beyond the public sector; the damage can affect private businesses, citizens and even national security. By partnering, government, the private sector and citizens can boost the nation's overall cyberdefense posture.

The stakes on cybersecurity couldn't be higher, but agencies shouldn't lose hope. Organizations that stay aware of the world around them are less likely to be surprised when cyberthreats reach their doorstep.

About GovLoop

GovLoop's mission is to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 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 the public sector.

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

govloop.com | @govloop

Thank You

Thank you to CenturyLink, Ciena, DLT, Fortinet, Red Hat and SolarWinds for their support of this valuable resource for public-sector professionals.

Authors

Mark Hensch, Staff Writer

Designer

Megan Manfredi, Graphic Designer

1152 15th St. NW Suite 800
Washington, DC 20005
P: (202) 407-7421 | F: (202) 407-7501
www.govloop.com
@GovLoop