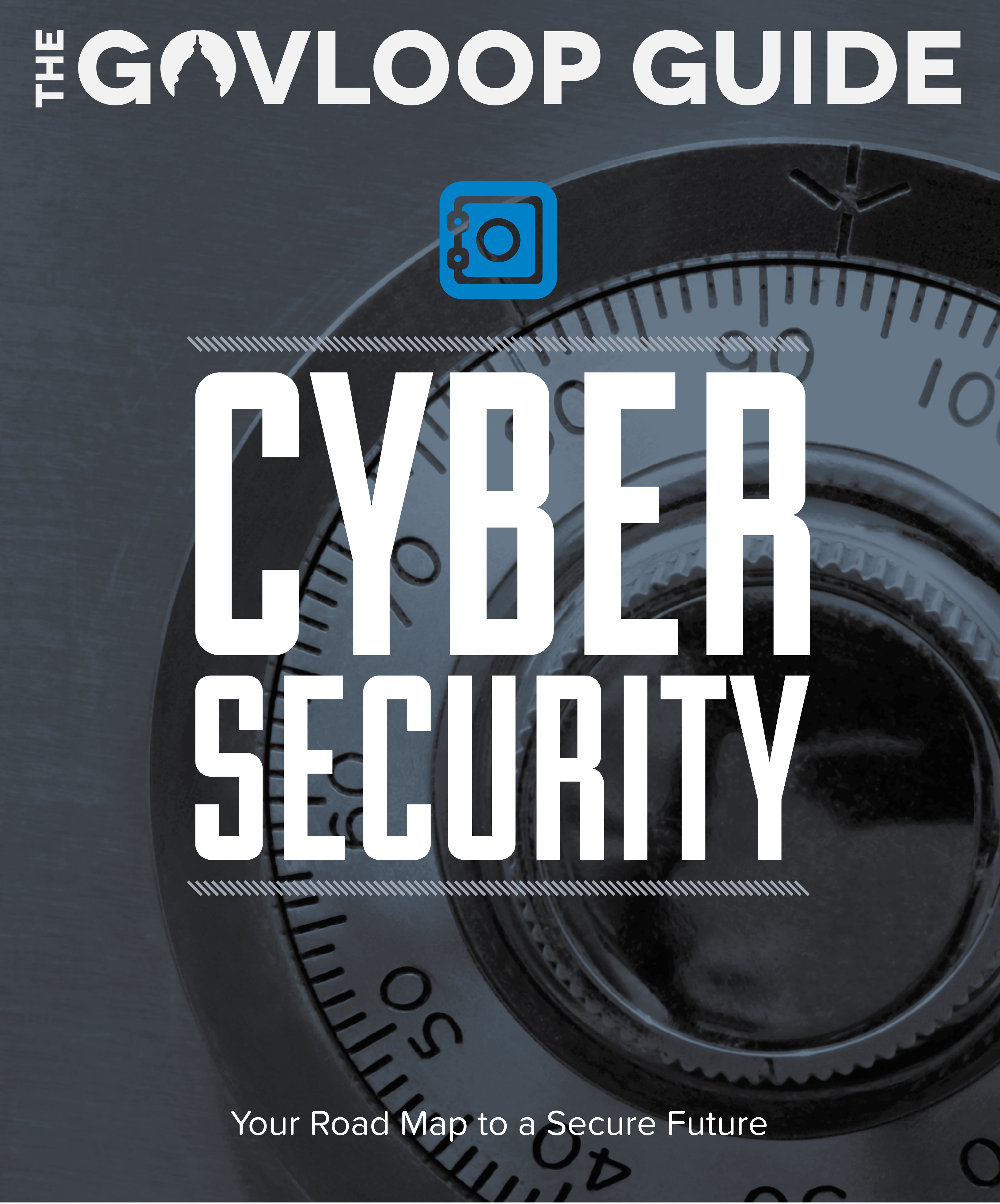
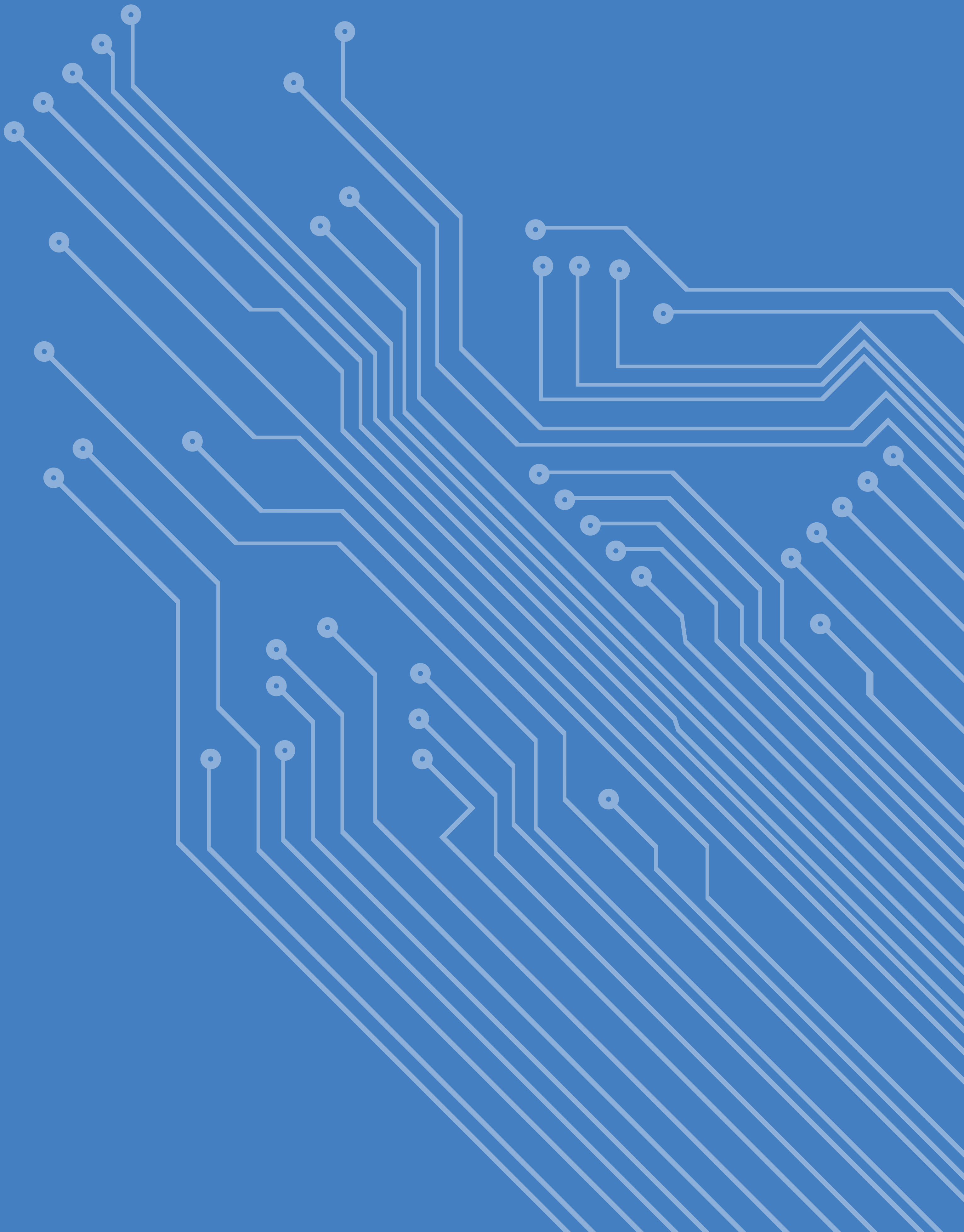


THE GOVLOOP GUIDE

CYBER SECURITY

Your Road Map to a Secure Future

INNOVATIONS THAT MATTER



CONTENTS

CYBERSECURITY:

YOUR ROAD MAP TO A SECURE FUTURE

In today's digital world, no organization is immune from cybersecurity threats. Whether it's Target, LivingSocial, the Federal Reserve or any other public-facing institution, every organization is at risk of having its data and infrastructure compromised. For security professionals today, being secure isn't just about thwarting attacks – it's also being prepared to react once you fall victim to a cyberattack.

Cybersecurity has certainly emerged as a key priority for information technology leaders. From the top levels of government, pressures have been increasing to protect U.S. critical infrastructure and collaborate across sectors. Both actions are essential components to improving the country's security posture.

The threat landscape has changed for cyber professionals. As government continues to collect, manage and store data, and as the number of mobile devices in the workplace grows, the number of target entry points has also substantially increased.

Meanwhile, owners of our country's critical infrastructure must now contend with cyberthreats in both the physical and virtual environments. "Critical infrastructure" is a term used to describe the electric grid, energy resources, telecommunication systems, water supplies and public health resources. For government agencies and the private-sector companies that operate under their jurisdiction, protecting our critical infrastructure is now a matter of our economic and social viability.

Training and educating the entire government workforce on proper cybersecurity protocol is a perpetual challenge. Cybersecurity efforts are not effective if they happen in a vacuum; it takes every employee doing his or her part to remain secure.

That's why GovLoop has released our latest report, "Innovations That Matter: Your Road Map to a Secure Future." GovLoop's "Innovations That Matter" series explores topics such as mobile, cloud, geographic information systems -- the latest trends and best practices shaping government.

Specifically, this report looks at:

- **Insights from 85 public sector cybersecurity professionals.**
- **An overview of the cybersecurity landscape.**
- **The importance of assessing your network to define cybersecurity policies.**
- **A case study from Daniel Durgin, chief enterprise security officer for the state of Maine.**
- **A case study from Quentin Hodgson, chief of staff for cyber policy at the Office of the Secretary of Defense.**
- **Best practices for assessing your network for increased security.**
- **A public-sector cybersecurity cheat sheet.**

Cybersecurity has changed the landscape of government, forcing state, local and federal governments to mitigate risk exposure and respond effectively to new and evolving threats.

This report starts by exploring the cybersecurity landscape for the public sector through results from a recent GovLoop survey.

EXPLORING THE CYBERSECURITY LANDSCAPE FOR THE PUBLIC SECTOR

GovLoop surveyed 85 public-sector professionals to explore the current state of cyber and the steps cyber professionals are taking to secure and assess their networks.

To structure the survey results, the National Institute of Standards and Technology (NIST) recently released the "Framework for Improving Critical Infrastructure Cybersecurity." It provides a high-level blueprint for addressing challenges and issues facing those in both the public and private sectors who are charged with governing our country's physical and virtual infrastructure.

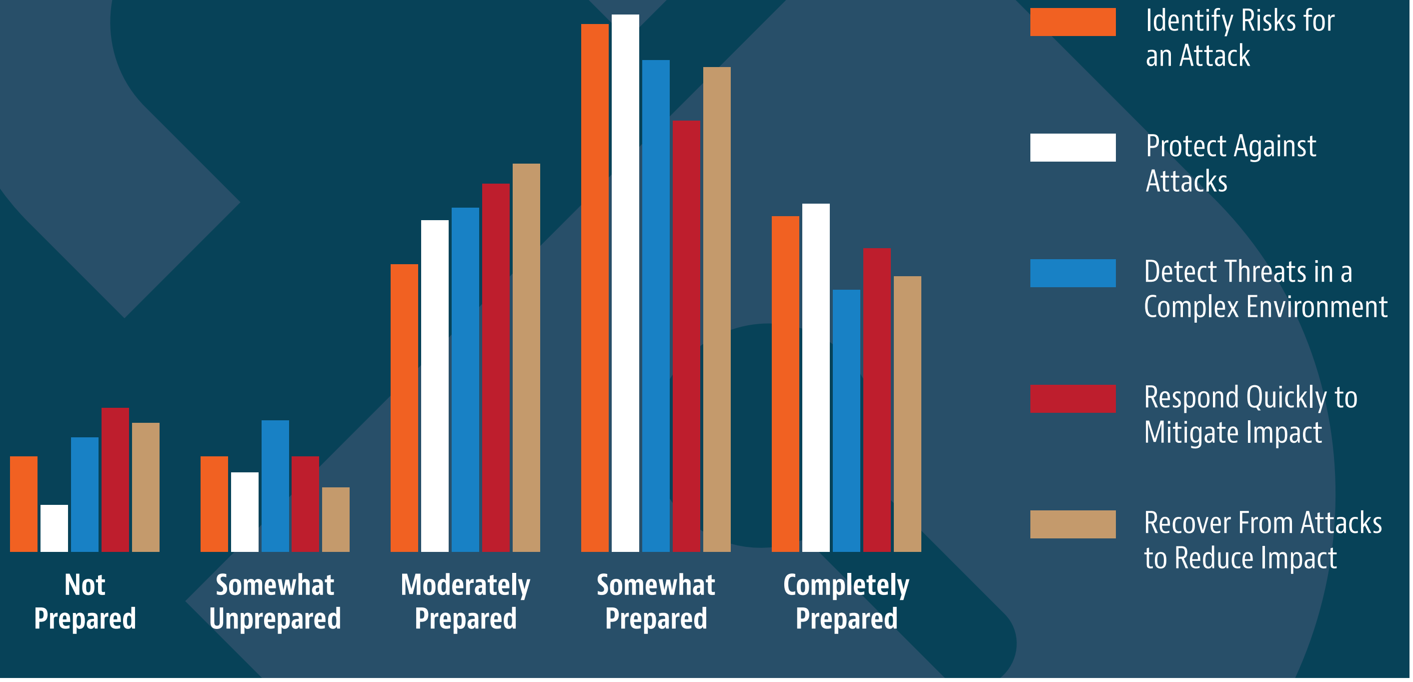
The report framework itself is a deliverable from the February 2013 "Executive Order — Improving Critical Infrastructure Cybersecurity." In that directive, the Obama administration tasked NIST with the development of a voluntary risk-based cybersecurity framework to help shore up cyber defenses. The NIST report breaks down the five essential steps of cybersecurity:

- **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.
- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired because of a cybersecurity event.

Figure 1 in our report explores government agencies' preparedness level for each of those components. Interestingly, for all five steps, respondents believe they are "somewhat prepared"

FIGURE 1. **How Prepared is Your Agency?**

On a scale of 1-5, with 5 being very prepared and 1 being not prepared, please rate your agency's preparedness level for the following:



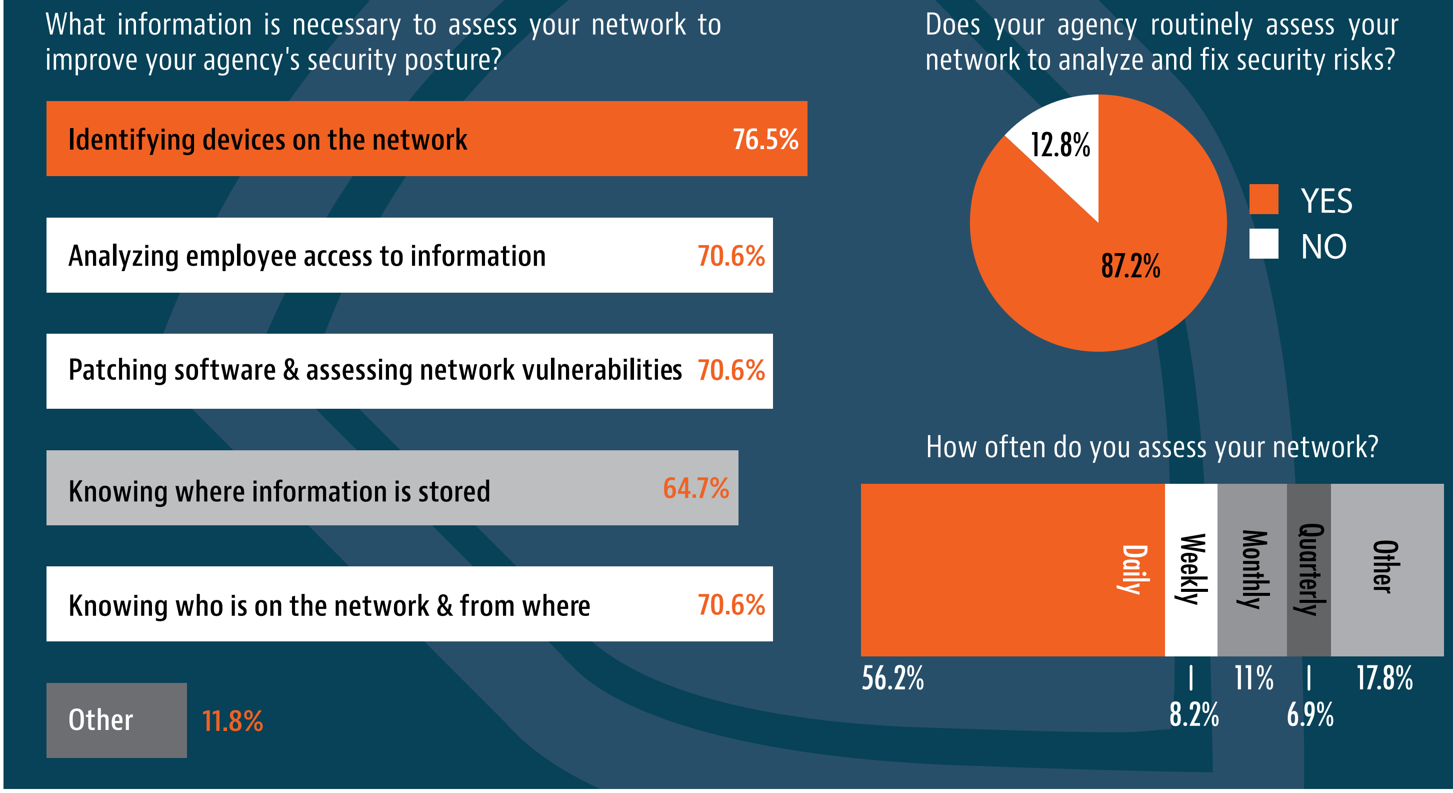
to combat an attack. Throughout this report, GovLoop has identified strategies and best practices for the "identify" stage, which NIST's framework breaks into five areas:

- **Asset management:** "The data, personnel, devices, systems and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy," the framework states.
- **Business environment:** This is essential because it helps an organization understand its mission, who important stakeholders are and what kind of services or assets should be prioritized.
- **Governance:** Governance is an important category across government IT. In particular to cyber, the policies, procedures and processes are critical for agencies to develop – and enforce. Without effective governance, organizations open themselves to risk and can't understand the vulnerabilities on the network.
- **Risk assessment:** Assessing the network allows organizations to understand the risk to their operations. By understanding the assets on the network and how they connect to people and processes, agencies can spot vulnerabilities and improve security.
- **Risk management strategy:** "The organization's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions," the framework states.

These five elements are just the beginning to fully assessing and protecting your network. Our best practices section builds on these essential categories.

Elaborating on this report's theme, Figure 2 explores what information is necessary to assess a network. At 77 percent, the leading response was "identifying devices on the network." Our survey also asked organizations how often they assess their networks to fix security issues. Eighty-seven percent of respondents said that they assess their networks, and 56 percent assess their network on a daily basis. (See Figure 2 for full results.)

FIGURE 2. **What Information is Essential to Assess Your Network?**



What information is necessary to assess your network to improve your agency's security posture?

Does your agency routinely assess your network to analyze and fix security risks?

How often do you assess your network?

An additional data point can be found in Figure 3, which explores the ways people may be accessing the network that could lead to a data breach. Using USB flash drives, accessing social media and cloud-based storage providers all expose an agency to risk. If these services are allowed, they must be accompanied by a proper governance strategy. This is an essential finding from the survey data.

In many cases, cybersecurity isn't only an IT problem – it's a data problem. Assessing the network means gaining an understanding of how data moves in your agency and enforcing policy. This includes investigating the many networks and Internet-facing networks you operate in addition to the physical transportation of sensitive information by the people who use it.

For instance, an employee may want to work on a spreadsheet after work hours. This person uses a flash drive to transport the document and accidentally drops the flash drive on public transit. The employee did not have malicious intent and may not have known he or she was breaking the rules.

The problem of assessing the network also ties in to the need to prioritize devices based on risk and to understand data assets. Once an organization understands its data – especially what is sensitive information – it can begin to create a risk assessment and response plan.

That second part is crucial to remaining secure. Figure 4 explores the essential components of creating an incident response plan. According to our survey, 56 percent of respondents currently have an incident response plan. Additional responses included:

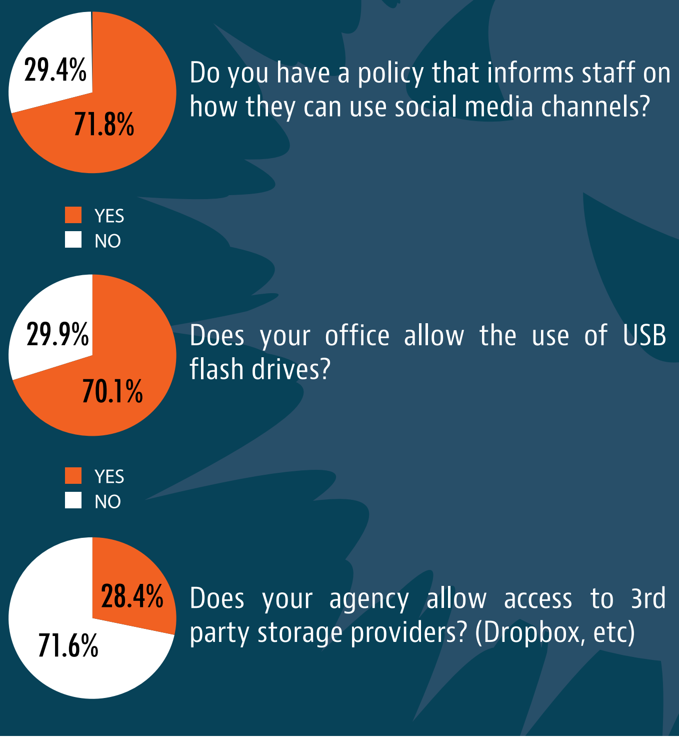
"Standard guidelines and protocols tailored to different threat areas."

"A very basic disaster recovery and continuity of operations plan exists that we try to update annually."

"It's tested; at least annually. Business impact assessment, recovery plan, communications plan, points of contact, legal requirements."

There's no reason government agencies should expose themselves to increased risk and vulnerabilities. This guide will continue to build on the ideas of proper asset management to help improve your cybersecurity posture.

FIGURE 3. **How are You Accessing & Sharing Information?**



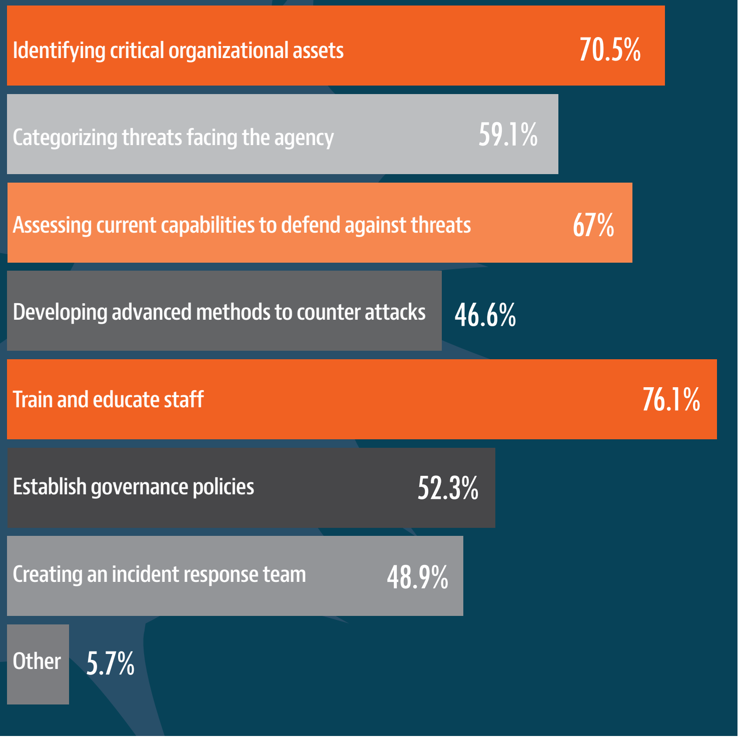
Do you have a policy that informs staff on how they can use social media channels?

Does your office allow the use of USB flash drives?

Does your agency allow access to 3rd party storage providers? (Dropbox, etc)

FIGURE 4. **What's Part of Your Response Plan?**

What elements are important to developing a response plan?



Dell Connected Security. Out-Connect The Threat.
In today's highly connected world, the threats are evolving faster than ever. Keeping security in individual silos just isn't enough anymore. Now you can out-connect the threat with Dell Connected Security, a new approach that shares intelligence between solutions for comprehensive protection across your IT environment. There may be thousands of scary-sounding threats out there, but Dell can help you out-connect them all. **Visit Dell.com/security.**

DELL

The power to do more

HAVE YOU SECURED ALL YOUR BASES? WHY UNDERSTANDING YOUR DATA IS ESSENTIAL TO SECURITY

It's not batting practice any longer for cybersecurity professionals. That time when your coach was throwing you lobs to help you work on the hitting mechanics? Things have changed. That's in the past.

In today's cybersecurity environment, you're being thrown everything in the pitcher's arsenal. Your opponents are relentlessly trying to gain a competitive edge and get ahead in the count. And if you've spent anytime in the cyber community, you know the playing field is far from controlled.

Securing your network means that it's up to you to anticipate your opponent's incoming move. More than ever before, you can't afford to whiff at the next pitch. The stakes are too high, and the consequences too grave.

"In reality, very few agencies take a proactive stance about sharing information between systems to correlate the different data pieces to share and render a better security solution," said Patrick Sweeney, VP of product management and corporate marketing, Dell. This sharing of information, he added, is imperative to gain insights on how to improve your security posture.

Crafting a better security solution comes as a challenge, as your cybersecurity portfolio probably includes solutions for perimeter security, remote access, and identity management, among many others. Each of these solutions has knowledge about the network and creates data as to how it operates.

But today, agencies are also being thrown another curveball to understand how to protect themselves: mobile.

"The tough two problems are: how to secure the [mobile] data when it is inside the perimeter, and how to let it out and stay in control of it when it is not inside the perimeter," said Sweeney.

"Everyone is hyper aware that data is leaving the perimeter," added Sweeney. "How do we retai ownership of it?"

One way agencies can think about how they can improve protecting data on their network is by answering this set of questions that Sweeney provides:

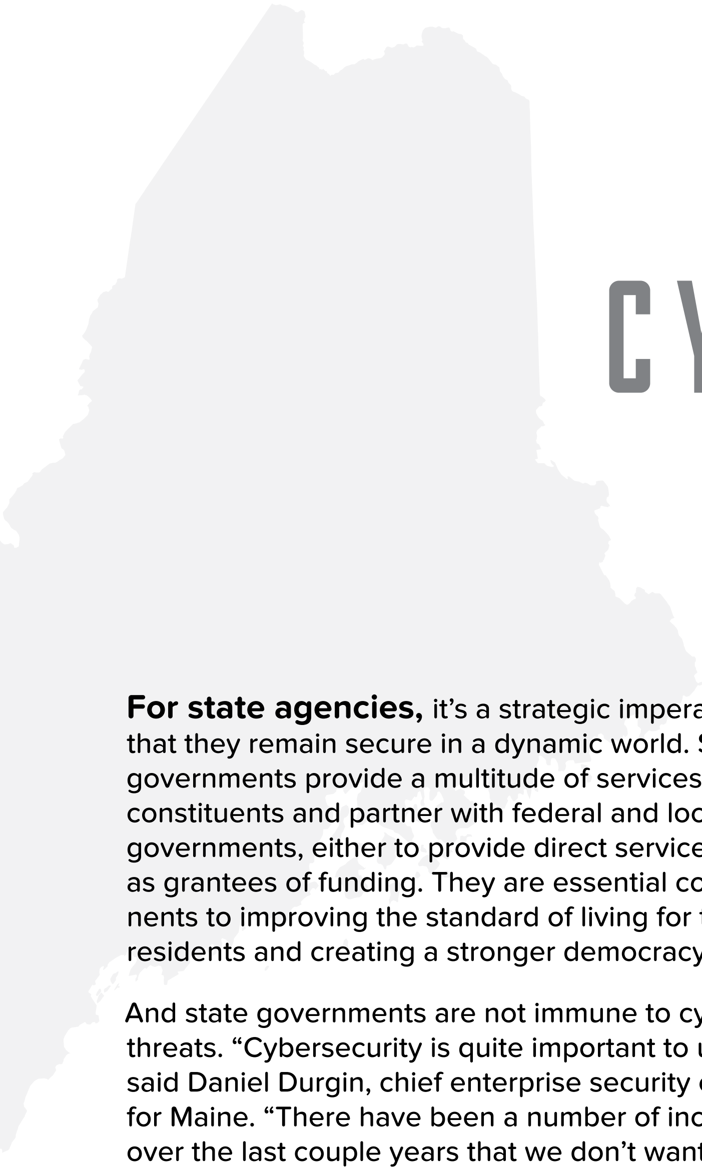
- **What is it that we are trying to secure?**
- **What kind of data is essential for users to have access to?**
- **Who needs to consume data and from where?**
- **Is it necessary for data to be accessible on mobile?**

Dell is working on these issues for themselves, too. They're taking a 360-degree view of security to help the public sector by addressing the four components below:

- **Embed security at the manufacturing of the device**
- **Acquire a robust security solutions portfolio**
- **Provide security expertise and build consultative relationships**
- **Remove silos and collaborate across the entire enterprise**

These four elements are essential to help you remain secure in a dynamic playing field. For government agencies, the key for network security is understanding how data moves on your network, and then deploying the proper security mechanisms to protect your agency.

Although you are challenged like never before, if you take initiative to understanding how your data enters and leaves your network, you'll be able to strengthen your cyberdefense.



A CENTER FOR CYBERSECURITY INNOVATION:

THE STATE OF MAINE

For state agencies, it's a strategic imperative that they remain secure in a dynamic world. State governments provide a multitude of services to constituents and partner with federal and local governments, either to provide direct services or as grantees of funding. They are essential components to improving the standard of living for their residents and creating a stronger democracy.

And state governments are not immune to cyber threats. "Cybersecurity is quite important to us," said Daniel Durgin, chief enterprise security officer for Maine. "There have been a number of incidents over the last couple years that we don't want to have happen to us, so cybersecurity is a huge topic and priority in the state of Maine."

To remain secure, Durgin defined three vital elements for governments:

- **Understand how an organization is hacked.**
- **Protect against social engineering, phishing and insider threats.**
- **Assure secure configuration of devices and patch software vulnerabilities.**

These three elements set the basis for security, and Durgin has coached his team to be aware of threats inside and outside the state.

"We are behind a firewall, but threats like phishing and malware quickly eliminate [the fact] that there is a firewall protecting us from the outside world," he said.

One of the major challenges that Durgin faces is the growth of mobile device use. With the number of devices increasing, the target has expanded in terms of risk and threats, he said.

"The threats and the motives are really wide now," Durgin said. "You do have greed, someone is just upset or it's a rogue state and this is an attempt to get at our government. If it has .gov at the end, it is a target to them."

> "**You need to take care** of the things that you can control . . . we're always doing assessments of one kind or another on the network."

– **Daniel Durgin,** Chief Enterprise Security Officer for the State of Maine.

PROTECTING & SECURING THE PINE TREE STATE

In order to navigate a quickly changing landscape of threats, Durgin and his team have designed numerous protocols and solutions. For instance, Maine has deployed a number of sensors that monitor traffic to state-run sites, allowing IT employees to quickly spot abnormalities and react.

"You need to take care of the things that you can control," Durgin said.

Additionally, his team routinely conducts log analyses, monitors traffic in real time and uses a process for identifying devices that are infected with malware or have become corrupted. Maine also has prioritized its assets and runs periodic assessments on devices.

"We're always doing assessments of one kind or another on the network," Durgin said. "Depending on the asset, it might be a monthly or quarterly assessment. We have a really good process in place that we call our deployment certification."

Additionally, anytime something new has been added to the network, the team runs penetration tests at the hardware and software levels. "We figure if the device is going to be open for business 24/7 on the Internet, we should take a good assessment, and secure it," Durgin said.

Not only is his team running assessments on new device points on the network, it also runs assessments on workstations to spot vulnerabilities.

One of the challenges to remaining secure is investing in the public-sector cyber workforce. Durgin has made sure to build a team that provides protection to the entire enterprise.

"The team that I manage that secures the state is pretty diverse," he said. "We have two folks that do penetration testing on applications and systems, and that's their whole focus. We also have people that manage perimeter security and also endpoint security."

Durgin also stressed the importance of collaboration and the need to share best practices and uses cases.

"Even if you're not a resident of Maine, I am a resource, and if you want to chat on the phone and see how we can learn from each other, I am definitely game for that," he said.

Cybersecurity efforts require a team effort and an enterprise-wide commitment. Under Durgin's lead, the state of Maine has become one of the leaders in cybersecurity and is working every day to adopt the latest technology and solutions to protect critical infrastructure and systems. In doing so, the state can assure its residents that it is delivering services efficiently and effectively.

Our next case study explores the Department of Defense's innovative approach to cybersecurity.

JUNIPer NETWORKS
THE THREAT ENVIRONMENT DEMANDS A NEW APPROACH TO DATA CENTER SECURITY
WITH A FOCUS ON AGILE ARCHITECTURE AND ACTIVE CYBER DEFENSE
Visit www.themodernnetwork.com/govloop

DEFENDING THE NETWORK THROUGH AN ACTIVE DEFENSE

Cyberdefense is at the top of every organization's priority list. Securing the network is the first line of defense to protecting critical information resources—the primary target for most threat actors. Chris Stoddard, Managing Director of Worldwide Security Sales with Juniper Networks – a recognized provider of innovative network solutions – discussed the importance of taking pro-active steps to defend Federal Government networks from cyberattacks.

"From our perspective, the network is the highway for all of the agency's sensitive data, and it is a critical component to protect," Stoddard said. "So when we talk to our customers, 'securing the network' often becomes job number one when it comes to considering the overall security posture of the agency."

Unfortunately, though network innovations have strengthened security operations, adversaries have developed correspondingly sophisticated tactics and continue to pose an increasingly significant threat to organizational data and infrastructure.

"No agency is immune to a potential attack these days," Stoddard said. "With advanced automation capabilities, hackers have seen the cost of intrusion and disruption greatly reduced. This means they're not only targeting big brand agencies and high-profile offices – they're also expanding to other vulnerable networks, regardless of size."

Therefore, Stoddard indicated that the tools and technologies for defense need to equal the rapidly-evolving threat environment. "The industry has been building bigger and bigger walls for as long as I've been in it," Stoddard said. "This approach doesn't always work given how intelligent the threats have become." This means that firewalls alone and signature-based detection methods may no longer be enough to hold the line.

One innovative solution organizations can implement stems from research conducted at Juniper Networks labs – a strategic approach they've developed known as 'active defense.' At the core of the active defense strategy are Juniper's best in class firewall, the SRX, Juniper Web App Secure, and Juniper DDoS Secure products.

An active defense, Stoddard explained, revolves around the notion of 'deception,' designed to help agencies identify and manage threats earlier in the attack cycle.   Identifying or disrupting an attack early in its life cycle causes more work for the attacking group, thereby disrupting the economics of hacking.

Juniper has pioneered a technique whereby network operators conduct deception by injecting fake code into the environment, serving as a minefield for potential intruders. This tactic allows operators to fingerprint the devices that malevolent actors use to gain unauthorized access or even to commit crimes against exposed Web applications. The objective is to arm network professionals with the capabilities to identify unwanted network visitors, verify their intent, and if desired, have the option to "fingerprint" and block the attacking device.

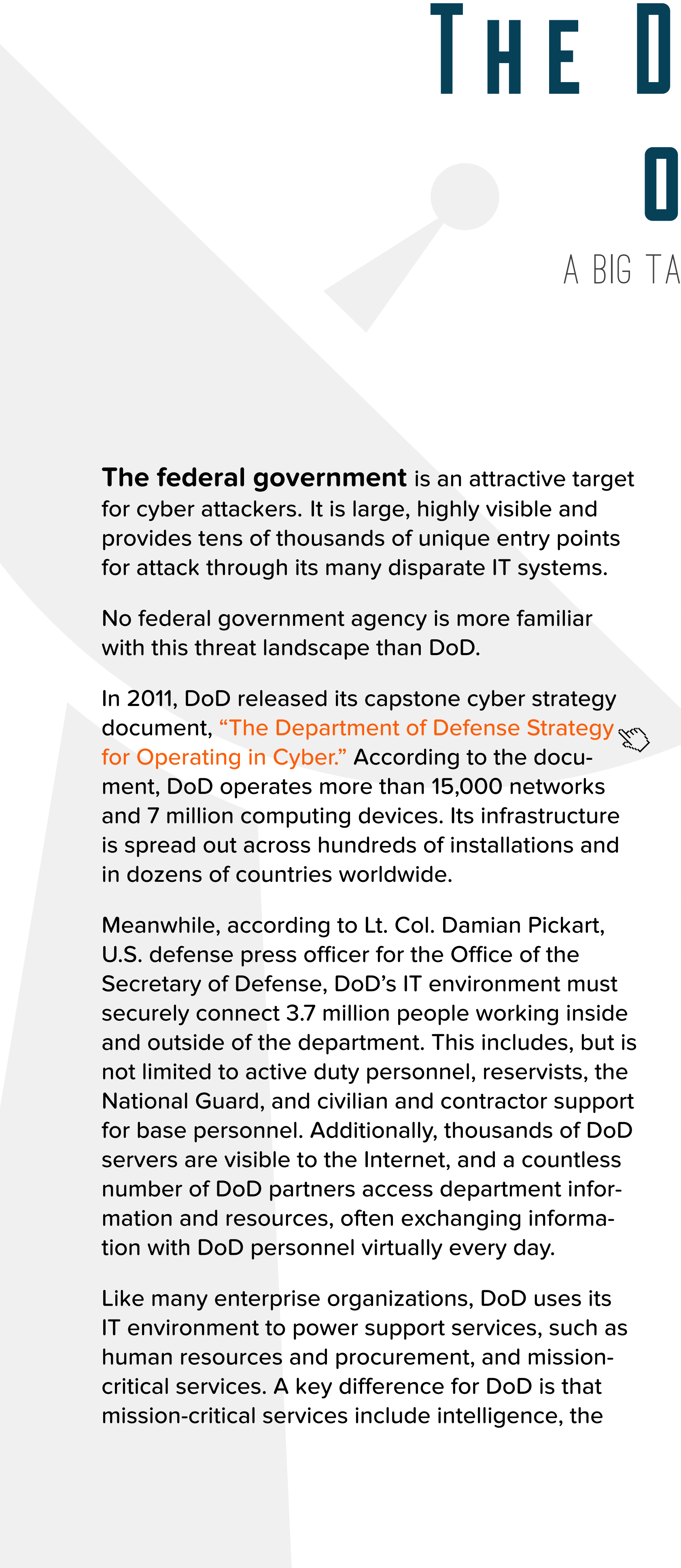
"Deception gives agencies two really important elements," explained Stoddard. "They are actually non-technical terms, but they are terms people care about: certainty and specificity."

With 'certainty,' the detection points or "tar traps" only will be touched by intruders, not by everyday users, enabling operators to be sure they are dealing with a potential threat. With 'specificity,' Juniper has developed an approach whereby operators can identify intruders down to the device, allowing users to post this signature to a Juniper-managed cloud service to share with other subscribers.

"That's the next stage in the evolution of [cyberdefense]," Stoddard said. "It is an ecosystem that enables IT professionals to collaborate and help one another in near real-time."

The Department of Defense:

A Big Target and an Even Bigger Solution



The federal government is an attractive target for cyber attackers. It is large, highly visible and provides tens of thousands of unique entry points for attack through its many disparate IT systems.

No federal government agency is more familiar with this threat landscape than DoD.

In 2011, DoD released its capstone cyber strategy document, "The Department of Defense Strategy for Operating in Cyber." According to the document, DoD operates more than 15,000 networks and 7 million computing devices. Its infrastructure is spread out across hundreds of installations and in dozens of countries worldwide.

Meanwhile, according to Lt. Col. Damian Pickart, U.S. defense press officer for the Office of the Secretary of Defense, DoD's IT environment must securely connect 3.7 million people working inside and outside of the department. This includes, but is not limited to active duty personnel, reservists, the National Guard, and civilian and contractor support for base personnel. Additionally, thousands of DoD servers are visible to the Internet, and a countless number of DoD partners access department information and resources, often exchanging information with DoD personnel virtually every day.

Like many enterprise organizations, DoD uses its IT environment to power support services, such as human resources and procurement, and mission-critical services. A key difference for DoD is that mission-critical services include intelligence, the movement of personnel and materials, and the command and control of the full array of military operations.

To compound this complex operating environment, the department reportedly receives 10 million attempted cyberattacks per day. The vast majority of these attacks are either unsuccessful or fail to disrupt the department's operations — but it only takes one significant breach to cause catastrophic damage to our country's defense architecture.

It is this potential scenario that has motivated DoD's response to cyberthreats. "We have to be concerned not just about the day-to-day threats that lead to the loss of intellectual property, but also the potential for a sophisticated adversary to do real damage to the United States through cyberspace," said Quentin Hodgson, chief of staff for cyber policy in the Office of the Secretary of Defense.

In short, the DoD IT environment is vast and its entry points varied and widespread. It's also the target of a range of threats, from smaller attempts by hackers in basements to sophisticated state-sponsored attacks by adversaries abroad. Given these characteristics, a bold, comprehensive response is needed. This response goes beyond shoring up password requirements or increasing the number of air gaps. It involves fundamentally changing the way DoD conducts the business of IT. This, among other reasons, has led to the creation of the Joint Information Environment (JIE).

THE JOINT INFORMATION ENVIRONMENT: A FRAMEWORK FOR DOD IT MODERNIZATION 🔒

JIE was launched in December 2012. According to documents released by the Office of the Secretary of Defense, JIE is a series of initiatives designed to migrate DoD's IT environment toward an enterprisewide, standards-driven and safeguarded environment. This will support department operations in a fully integrated manner.

According to a recent speech by Adm. James Winnefeld, vice chairman of the Joint Chiefs of Staff, JIE includes networked operations centers, core data centers and a global identity management system with cloud applications and services. JIE's primary goals are to remove barriers to information sharing, promote collaboration and interoperability across the department and with non-DoD mission partners, and enhance DoD security against cyberthreats and vulnerabilities.

"We are trying to establish a common and single security architecture for DoD networks writ large so that we can reduce the unique nature of individual networks, especially in those networks where we may not have good insight into what is happening," Hodgson said.

In other words, the diversity of DoD's networks, coupled with the reality that not all networks are tracked all the time, provides soft spots in the IT environment. These areas may provide openings for cyberattacks, which can spread to critical networks or data centers.

"Having that baseline – setting those standards across the department – will help us improve and migrate towards a defensible architecture," Hodgson added.

A secondary goal is make the DoD IT enterprise more efficient, cost-effective and smarter. This means the department is seeking to simplify, standardize, consolidate and automate its IT infrastructure – a core feature of JIE. It attempts to merge separate initiatives – mission efficacy, cost efficiency and security – into a unified approach that reaches across the spectrum.

Here's an example of how JIE works. DoD is actively working to reduce the number of data centers from 2,000 to 100. The department is also collapsing the number of Internet access points within its IT environment. Moreover, Hodgson said DoD is retiring aging legacy systems, which serves two complementary functions. First, upgrading operating systems to new instantiations addresses underlying vulnerabilities

that may have persisted without modernization. At the same time, decommissioning aging systems can also reduce drag on the department due to costly maintenance requirements – frequently because the original vendor no longer supports the product.

JIE: A FRAMEWORK, NOT A PROGRAM

It is important to note that JIE is not a specific program with an official funding line or a specific solution to one particular cyberthreat or IT vulnerability. Therefore, although decommissioning and legacy replacement are in some cases the appropriate prescription, the overall goal is to continue leveraging existing programs, including technical refresh plans and acquisition processes. The difference is that now these component programs will operate under the auspices of the standards JIE established.

The intention is to create a framework that is flexible and adaptable to changing conditions. This includes acclimating to new network warfare requirements, a change in DoD's budget allocation and, most pertinent to this report, the constantly mutating nature of cyber threats.

In many ways, pursuing a framework that is standardizing and flexible seems fundamentally incompatible. Yet this is perhaps the defining feature of our contemporary defense infrastructure, both in the physical and virtual worlds.

"We are not a homogenous organization," Hodgson said. "We have services, we have combatant commands, we have military units out there. We have different agencies with different missions."

This poses extreme difficulties for implementing any enterprisewide solution, which highlights JIE's importance. For example, by providing standardization across the enterprise through a single security architecture, new solutions may be implemented fasvter, especially if weak spots and vulnerabilities are phased out of the environment. Furthermore, through the development of common engineered solution designs, key programs can be scaled up or adapted to numerous purposes, all while operating under a standard cybersecurity measurement.

A PROGRAM IS ONLY AS GOOD AS ITS PEOPLE

JIE is a significant step toward achieving in the virtual world what the military has already accomplished in the physical.

"Our transition to JIE constitutes a new level of jointness in IT, akin to the higher levels of jointness we've achieved in other areas," Winnefeld said.

This will certainly strengthen DoD's security posture as it defends against the onslaught of virtual attacks it receives daily.

At the same time, this is not the only tool in the department's arsenal. Hodgson reinforced DoD's commitment to its personnel.

"You have to be active on your network," Hodgson said. "At the end of the day, having really good analysts – people who are looking at the network and understanding the mission, so that they understand what looks unusual on the network – is a really important piece of this strategy."

> “**We are trying** to establish a common and single security architecture for DoD networks”
>
> – **Quentin Hodgson**, Chief of Staff for Cyber Policy in the Office of the Secretary of Defense

YOUR CYBERSECURITY FOUNDATION: ASSET MANAGEMENT

Why asset management is the first step in improving your security posture.

Would you ever consider living in a house without knowing where all the entrances are? Or not having all the keys and knowing who can enter your home?

Probably not. No one would want to live in that kind of environment – you'd be in constant fear. Just like needing to know who can enter and exit your home for your personal safety, you must understand who, what, when, and how devices are accessing your network to improve your security posture.

That's why asset management is essential to keeping government infrastructure safe and secure. NIST describes asset management as being when "the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy."

"If you don't have good asset management you'll never get your arms around the baseline for your security," said Scott Montgomery, chief technology officer of McAfee. "Because if you have a mechanism that you can't account for, then they are not part of your security posture, they are not part of your security plan."

The implementation of asset management has become increasingly important, especially as we've seen mobile technology explode. The Pew Research Internet Project states that 90 percent of American adults have a cell phone, while 58 percent have a smartphone. And mobility has now extended beyond cell phones; Pew also reports that 42 percent of American adults own a tablet.

"Mobility is definitely a game changer because you are not carrying a phone around anymore," said Montgomery. "You're carrying a computer that has the ability to make telephone calls."

The computing power of devices and the ease with which you can share information on them has inevitably led to increased risks for government. But Montgomery cautions agencies to not think just about the device – they must also focus on the data.

"At the end of the day, knowing where the data is, knowing who has access to data, how it can be manipulated, how it can go in and out of a particular network or environment is going to be more important than what mechanisms people have to carry it in and out," said Montgomery.

"If you always track the data," he added, "you are going to be in a security posture [more] than if you try to keep up with the onslaught of IP enabled devices."

Montgomery reminds us that the three keys to information security are confidentiality, integrity and availability. Starting with effective asset management is the best way to achieve these means.

> **Mobility is definitely a game changer** because you are not carrying a phone around anymore … You're carrying a computer that has the ability to make telephone calls.

– **Scott Montgomery**, Public Sector Chief Technology Officer, McAfee

SOPHIA LOADED
MOUSE X: 1 Y: 287

Best Practices for Asset Management

Case studies from Maine and DoD provide hope for agencies looking to protect the networks and data centers that support mission-critical operations. These innovative practices did not come without challenges – obstacles not unlike the three our survey highlighted that government is facing. We explore these below, along with best practices to assess and identify assets on your network.

One challenge that came up in the survey is that agencies are operating in a dynamic threat landscape. “Our adversaries are quick to change and adapt threat tactics,” one respondent said. Hazards extend internally and externally and include everything from malware to phishing.

“We operate in a constantly changing threat landscape,” another respondent said.

Second, as threats continue to grow in complexity, resources continue to shrink. To remain secure, agencies must have the appropriate resources and staff. Yet in many cases, agencies are lacking cybersecurity experts or resources. One survey respondent who cited a lack of resources dedicated to information security echoed the thoughts of many across government about one of their challenges.

A final theme from our survey was the need for improved governmentwide collaboration. “Large state agency with multiple sites that are not well integrated” was an issue one respondent noted. Another cited “managing multiple devices that access the network both locally and remotely.”

Although challenges certainly exist, best practices are available as guidelines to agencies to improve the way they assess their networks and provide protection. Our survey and interviews with cyber experts produced 10 best practices. They are by no means a finite list, but they provide a starting point for how to improve your network’s resiliency.

1. Develop an Inventory of Devices.

Our survey respondents noted the importance of having an inventory of devices, as indicated by comments such as “Be aware of what you have, who's using the technology and why” and “Daily checks and constant communication with our IT department.” Hackers are looking for devices that come on and off networks, which have outdated security patches and software vulnerabilities. By having an inventory of devices, you can assess the state of your network and be able to quickly patch vulnerabilities and identify abnormal activity. “Understanding your network is critically important,” DoD’s Hodgson said, “but it is more than just understanding what you have. It is also about understanding how you are using [your IT infrastructure] and identifying the most critical pieces.”

2. Protect Across All Platforms.

Whether it’s mobile devices, laptop computers, workstations or tablets in the field, attackers have no preference. They are just looking for where your agency is exposed. It’s essential to monitor and protect across all platforms, and reduce vulnerability. To those ends, your agency must adopt a solution to track and monitor all devices and have protocols in place to quickly remediate corrupted devices.

3. Conduct Routine Assessments.

Routine assessments are essential to securing your network. Survey respondents suggested ways to perform them. For instance, one participant proposed conducting annual or quarterly reviews of issues and how those issues are being dealt with. Another recommended “periodic reassessments, taking into account recent changes in threats and known vulnerabilities.”

A third respondent said different groups conduct consistent vulnerability scans and penetration testing at least every 90 days at his or her agency. It also uses layered security approaches to include both physical and cyber, and "better control over the budget, and better training and awareness on a monthly basis for all employees from the top down and bottom up."

4. Control Accessibility to the Network.

It's essential to control access to the network. This means having secured passwords, and if necessary, restricted access based on the user profile. Although these basic fixes do not provide absolute security, they make it one step harder for an intruder to access your network.

5. Establish, Enforce and Train Employees on Governance Policies.

Cybersecurity requires everyone across the enterprise to understand and be trained on proper uses of devices. This means documentation on how to use flash drives, accessing information in the cloud and role-based access for materials. The challenge here is finding the right balance between security and allowing employees to remain productive.

"The biggest challenge is avoiding the implementation of security practices that become increasingly burdensome on the ordinary, day-to-day user of network systems and data," Hodgson said. "That is the key piece – giving them the tools to be operationally efficient and secure at the same time."

6. Show Data and Communications Flows Across the Agency.

Once organizations understand the devices and tools accessing the network, the next step is to understand how information moves among devices and networks. Knowing how data flows is crucial to understanding how to protect it and the network.

Additionally, it's important to examine when and where it is appropriate to segregate key elements of your data infrastructure from the rest of your networks, which can cause tension.

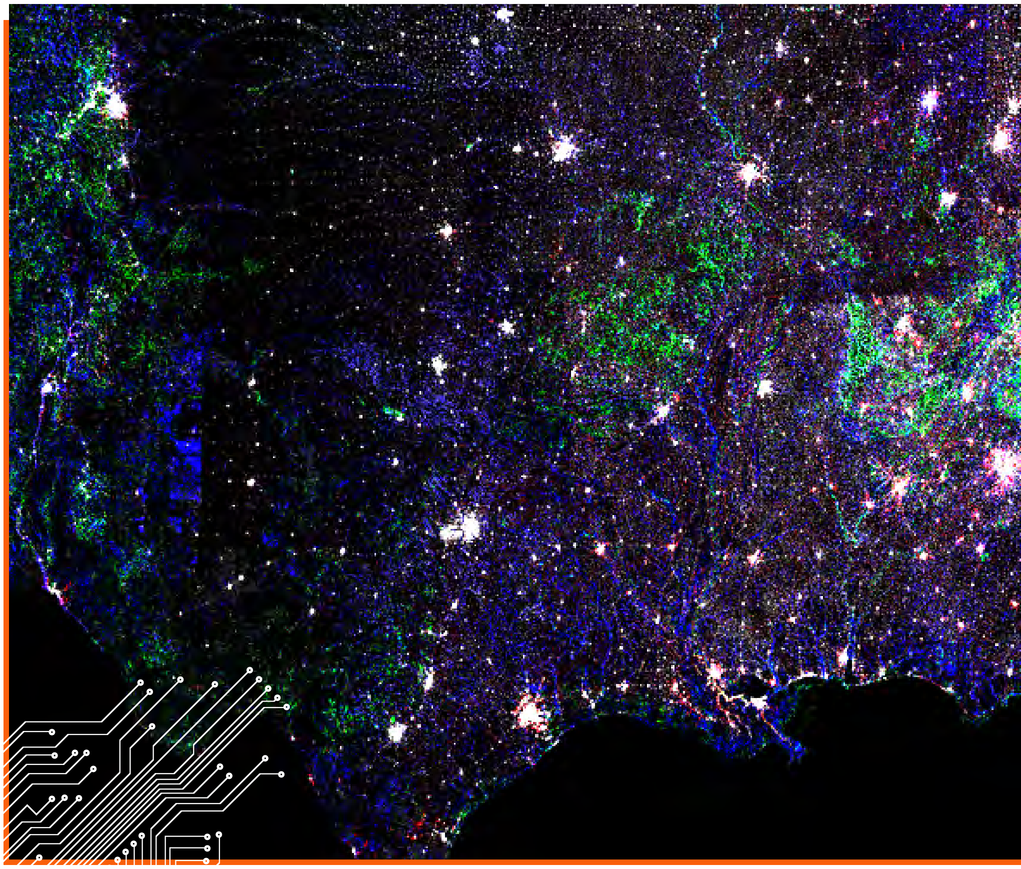
"We've found the goodness in sharing information, but we've also found that it opens us up to vulnerabilities, whether it is from an insider threat, but also from an external threat who may get access to that information," Hodgson said.

7. Prioritize Your Data Assets.

Government collects a lot of data, but not all of it needs the same level of protection. Agencies should assess and protect high-value data sets and information first. This begins with an assessment of your core mission objectives.

"You have to start with mission – what are you trying to achieve, strategic objectives, what are you working towards – because without understanding that, you could get lost in trying in to address every single vulnerability that may be out there," Hodgson said.

Agencies can save time and energy by knowing the critical data assets within the organization, who accesses the information and how they access and build systems to adequately protect information.



This is the foundation of a sound cyber risk management strategy.

"The thing we have to come to grips with in any enterprise is that trying to prevent everything equally everywhere is not going to be possible," Hodgson said. "You have to make choices about what you need to continue conducting your business and what are the things that don't need quite as much attention."

8. Share Information About Risk.

"Ensure that the right stakeholders and subject-matter experts participate in the assessment to ensure that every aspect and detail is adequately covered," a survey respondent said. This insight reinforces the need for improved collaboration inside and outside public agencies, and it helps us realize that ours is a shared risk when it comes to cybersecurity.

"Collaboration is critical. We don't have a monopoly on the type of threats that we face, and certainly the U.S. government writ large does not have a monopoly," said Hodgson, noting that DoD has discovered real benefits in its relationships with its defense industrial-base partners in the commercial sector.

9. Integrate Your Cybersecurity Strategy Into Your Overall IT Strategy.

This is what DoD is doing as it migrates toward JIE. The department discovered that other IT initiatives, such as efficiency and streamlining, went hand in hand with its cybersecurity measures. Integrate your cybersecurity plan – beginning with the assessment of your IT infrastructure – into your plans to modernize and decommission aging, legacy systems. You may discover that your requirements are aligned across the entire spectrum.

"We are making sure that we are retiring legacy applications that are a heavy drag on the department in terms of upkeep or because the vendor no longer provides support, but also because through upgrading and migrating operating systems to newer instantiations, we are able to address those underlying vulnerabilities that may have persisted," Hodgson said.

10. Prioritize Risk Responses by Asset.

Once assets have been identified, your organization should arrange them based on level of importance. By prioritizing your assets, you will be able to respond faster in a crisis.

Finally, one survey respondent provided an overview of the best practices for asset management:

1. **Identify critical assets and the risks/possible threats.**
2. **Evaluate compliance and policy measures.**
3. **Assess existing controls, especially user access controls.**
4. **Analyze vulnerabilities and areas of concern.**
5. **Have contingency plans in place as part of remediation efforts.**
6. **Exercise continuous monitoring.**

These best practices provide you with a great starting point to examine your cybersecurity procedures. Still, it's important to remember that cybersecurity is everyone's responsibility.

"IT security isn't just all IT, which is IT vendors," said Maine's Durgin. "Our users are part of that equation and we need to get them on board."

To remain secure, it takes an effort that extends across the enterprise, is guided by leadership and has the commitment of all employees.

That's a lot to digest. Don't worry about remembering it all. To conclude our guide, we have provided you with a public-sector cheat sheet on cybersecurity. 🔒

SURVEY SHOWS BOTH HACKERS & AGENCY INSIDERS ARE TOP CYBER THREATS

Recently, SolarWinds and Market Connections surveyed 200 IT and security professionals in the federal government and military. The survey found that 94 percent of respondents said their agencies' cybersecurity readiness is either good or excellent. However, though federal IT pros believe they're ready to thwart attacks, the survey did reveal that numerous threats still remain. The biggest danger may surprise you:

"The survey clearly shows that people are the biggest cyber security threat – whether agency insiders or intruders," said Chris LaPoint, VP product management, SolarWinds. The survey reports:

- **50 percent of respondents cited external hacking as the top cyber threat for federal agencies**
- **29 percent noted threats from insider data leakage and theft**
- **20 percent reported stolen mobile devices as a security risk**
- **18 percent cited physical security attacks as a menace to security efforts**

Threats plague federal agencies from both external malicious intruders like hackers – and from careless or untrained insiders. So what can a federal IT pro do to mitigate these human threats to security? Survey data shows that federal IT pros are challenged to implement the right monitoring and detection technologies and to provide adequate training to educate employees.

"It is extremely difficult to change human behavior. People may have the best intentions, but it's really hard to reach 100% of the people and make sure they are 100% compliant," said LaPoint. "And while training is important, IT pros need the right tools to assess compliance and implement proactive and active controls to prevent people from basically shooting themselves in the foot."

For government agencies, continuous monitoring has served as a way to safeguard against threats, remain compliant and identify vulnerabilities. The survey found that two-thirds of respondents have adopted at least one continuous monitoring solution and the majority of participants believe a continuous monitoring solution has a positive return on investment.

Those who have deployed continuous monitoring have also been able to reduce the amount of time it takes to respond to those security events or issues. For example, the survey reports that 46 percent of users can detect rogue devices on the network in minutes, compared to 23 percent of non-adopters of continuous monitoring solutions. Additionally, 30 percent of agencies that have adopted continuous monitoring solutions can detect when firewall rules are out of compliance within minutes, compared to 16 percent of non-users.

"Continuous monitoring of networks, systems and applications provides federal IT pros critically important data and insight into the health of their IT infrastructures, empowering them to take the necessary steps to prevent any cybersecurity breaches. SolarWinds IT management software can help agencies implement the right monitoring controls to neutralize human threats and remain secure."

For over 10 years, SolarWinds has been supporting government with both free tools and products.

"Our products are built on the principle of collect once, and report many," explained LaPoint. "Whether it is log or firewall management, server or application monitoring, network management, or patch management, the solutions are built to serve the needs of both IT operations and information security professionals within organizations."

SolarWinds provides IT management and monitoring solutions to help government agencies remain secure and compliant. They offer solutions for continuous monitoring, cybersecurity, network operations, compliance, data center consolidation, cloud computing, mobile workforce and devices, and scaling to the enterprise.

SolarWinds software is available on the U.S. General Services Administration (GSA) Schedule, Department of Defense ESI and other contract vehicles. Visit SolarWinds' Government Solutions page for more information including fully functional free trials of products or visit SolarWinds' community, thwack, to download 300 free out-of-the-box compliance report templates of major auditing authorities including DISA STIG, FISMA, and NIST.

Your Cyber Cheat Sheet

LOOKING TO GET
SMART FAST ON
CYBERSECURITY?
LOOK NO FURTHER.

Mini-Glossary

- **Access Control Mechanism:** Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system.

- **Account Management, User:** Involves 1) the process of requesting, establishing, issuing, and closing user accounts; 2) tracking users and their respective access authorizations; and 3) managing these functions.

- **Critical Infrastructure:** Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.

Must-Reads

(Click a title to open in browser)

- **Framework for Improving Critical Infrastructure Cybersecurity**
- **Executive Order — Improving Critical Infrastructure Cybersecurity**
- **Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges**
- **Agency of the Future: Winning the Cybersecurity Battle**

5 Key Components of Cybersecurity

- **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.
- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired because of a cybersecurity event.

What information is necessary to assess your network to improve your agency's security posture?

Identifying devices on the network	77%
Analyzing employee access to information	71%
Patching software & assessing network vulnerabilities	71%
Knowing where information is stored	65%
Knowing who is on the network & from where	71%

ATTACK!

What kind concerns you the most?

49% **VIRUSES** A program that copies itself and infects a computer without the permission or knowledge of the user. It can corrupt or delete data, use e-mail programs to spread itself to other computers, or even erase a hard disk.

49% **PHISHING** A digital form of social engineering that uses authentic-looking but fake e-mails to request information from users or direct them to a fake website that requests information.

38% **TROJAN HORSES** A program that appears to have a useful function but also has a hidden and potentially malicious function. It evades security mechanisms by masquerading as a useful program that a user would likely execute.

27% **DENIAL-OF-SERVICE** A computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.

26% **DISTRIBUTED DENIAL-OF-SERVICE** A variant of the denial-of-service attack that uses numerous hosts to perform the attack.

From the Experts

> "We are behind a firewall, but threats like phishing and malware quickly eliminate [the fact] that there is a firewall protecting us from the outside world."
>
> – **Daniel Durgin,** Chief Enterprise Security Officer for the state of Maine.

> At the end of the day, having really good analysts – people who are looking at the network and understanding the mission, so that they understand what looks unusual on the network – is a really important piece of this strategy."
>
> – **Quentin Hodgson,** Chief of Staff for Cyber Policy at the Office of the Secretary of Defense.

☑ 10 Best Practices for Asset Management

- Develop an Inventory of Devices.
- Protect Across All Platforms.
- Conduct Routine Assessments.
- Control Accessibility to the Network.
- Establish, Enforce and Train Employees on Governance Policies.
- Show Data and Communications Flows Across the Agency.
- Prioritize Your Data Assets.
- Share Information About Risk.
- Integrate your Cybersecurity Strategy Into Your Overall IT Strategy.
- Prioritize Risk Responses by Asset.

YOUR PATH TOWARD ADOPTING CONTINUOUS MONITORING 🔒

A conversation with Jennifer Nowell, Sr. Director, Strategic Programs - US Public Sector, Symantec.

Why is adopting continuous monitoring solutions an important step for government agencies to improve their security efforts?

The reason it is so critical is because it provides the confidence that you have a baseline level of security for every agency. Then, as we drill down to the specific agency, it provides them the confidence that they know the risk tolerance. On a more regular basis, they understand the level of security that they have in their environment.

Who should be involved in the continuous monitoring process?

From an industry perspective, as we talk to CIOs or CSOs, our attempts to tackle continuous monitoring has taken us to other parts of the organizations, such as the operational side. This is because if we find problem areas, we need to work with our business counterparts to fix what we find.

In addition, I've learned that [continuous monitoring] is a true matrix ecosystem. When we think about all of the pieces and parts needed to run an effective mission, there are so many different dependencies on those systems. Consequently, it is everybody's problem and everybody's business.

What are the challenges to adopt continuous monitoring?

The top challenge is to hire, train and retain talent. Agencies are struggling with keeping their analysts and creating a clear plan for them to feel successful. It really comes back to the people. We're figuring out the process and the technology – that will continue to evolve. But the people part tends to be the hardest part, especially as many keep shifting to private industry. We need to come up with a solution to retain and grow talent, because civil service is very important to our nation.

What are some best practices for continuous monitoring?

I would advise agencies to follow the cybersecurity framework. When you look at the fundamentals, knowing where your hardware and your software assets are ensures that you are monitoring those assets in the event of a change. You are ensuring that there is no drift in the configuration. You also need to do vulnerability scans to ensure that the software you have running doesn't have any holes. For example, you've just upgraded your operating system or application and now you have a new gaping hole you didn't know about yesterday. Those fundamental components within the current Continuous Diagnostic Mitigation (CDM) program are the first correct steps.

How can Symantec help agencies improve their cyber security posture?

Symantec is a CDM tool provider. We provide the technical tools answer to many of the best practices outlines for agencies. Our role is to help agencies and organizations in areas where they have gaps. It can be very tool-centric, such as when organizations use a specific tool to fill a specific gap. But it also can be more complicated. It can be as intricate as aggregating all information or associating the risk with their central mission.

From small to large, Symantec can play a part in helping agencies get to a place where they understand those CDM best practices, know how to apply those best practices to their operations, use the appropriate toolsets, and get to that place where they have visibility into their relative levels of tolerance.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 100,000 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 Pat Fiorenza, Senior Research Analyst, GovLoop, at pat@govloop.com, or follow him on Twitter: @pjfiorenza

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

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

www.govloop.com
Twitter: @GovLoop

ACKNOWLEDGEMENTS

Thank you to Dell, Juniper, McAfee Software, Solarwinds, and Symantec for their support of this valuable resource for public-sector professionals.

Authors: Patrick Fiorenza, senior research analyst, GovLoop, and Adrian Pavia, research fellow, GovLoop

Designers: Jeff Ribeira, senior interactive designer, GovLoop, and Tommy Bowen, junior designer, GovLoop

Editors: Steve Ressler, president and founder, GovLoop, and Catherine Andrews, director of content, GovLoop

1101 15th St NW, Suite 900
Washington, DC 20005
Phone: (202) 407-7421
Fax: (202) 407-7501