YOUR CYBERSECURITY CRASH COURSE

INNOVATIONS THAT MATTER

Strengthening the Security Posture of Government Networks

Carahsoft is pleased to support the government's CDM and cybersecurity initiatives through its partnership with a broad range of technology manufacturers, resellers and system integrators.

Akamai Cloud Security Solutions	AlertEnterprise! Security Convergence Solutions	CORE SECURITY Intelligent Network Visibility Platform	CYBERARK Privileged Account Controls & Monitoring	EMC² Secure On-Premise Storage Infrastructure
ExtraHop Wire Data Analytics Platform for Continuous Monitoring	f5 Application Security Testing & Management	FireEye Cybersecurity and Malware Protection	Gigamon Intelligent Network Visibility Platform	hp Integrated Enterprise Security Solutions
HYTRUST Cloud Under Control Virtualization Security, Compliance & Control	IMPERVA Data Center Security Solutions	Infoblox CONTROL YOUR NETWORK Automated Network Control	invincea Endpoint Security Solution	MarkLogic NoSQL Platform for Cyber Defense & Analysis
mongoDB Cross-Platform Database for Big Data Analytics	pentaho Real-Time Predictive Analytics	Ping Identity Identity & Access Management Solutions	redhat SE Secure Linux	RSA Security, Risk & Compliance Management
SafeNet The Foundation of Internet Security Data Protection & Software Monetization	servicenow Cloud Infrastructure Security Platform	splunk> Operational Intelligence Software	ssh COMMUNICATIONS SECURITY Data-in-Transit Security Solutions	Symantec Monitoring, Remediation & Compliance Reporting
tripwire Security Configuration & Vulnerability Management	Trustwave DbProtect Database Security & Audit Logging	VENAFI Next-Generation Trust Protection	vmware Network Virtualization & Security Platform	Vormetric Data Security Simplified Enterprise Encryption & Key Management

Carahsoft's solutions are available through a large ecosystem of reseller and system integrator partners and through a variety of contract vehicles including GSA Schedule 70, SEWP-V, CMaaS BPA, and others.

cybersecurity@carahsoft.com carahsoft® Please call us: 888.662.2724

© 2014 Carahsoft. All rights reserved.

EXECUTIVE SUMMARY

In 1988, Robert Tappan Morris became the first person to be convicted under the U.S. Computer Fraud and Abuse Act. Curious about how big the Internet was, Morris wrote a script now known as the "Morris worm." He never intended to inflict harm to machines, but as the worm replicated and spread throughout the Internet, networks slowed, crippling computers.

The Morris worm would serve as a preview of a world to come, and agencies have placed a strong emphasis on cybersecurity and cyber controls at their agencies ever since.

We live in a hyper connected world, where information technology administers must reconcile the need for modernization against the significant security risks posed by IT deployment. Today, data can be transferred through a variety of IT services, including cloud, flash storage, e-mail or even printed copies. Regardless of the technology, data security requires a concerted effort to take a holistic approach to information management.

At GovLoop, we see information security as the defining challenge of this era of government: How can government meet security demands against modernization? This is by no means an easy task and, unfortunately, it does not yet have a definitive solution.

But this guide will challenge you to build a culture of cybersecurity. We're calling on you to be cyber champions, to learn the best ways to communicate cybersecurity needs across your agency. This guide will help you think about larger cybersecurity trends and create an environment that has the agility to respond to new and emerging threats.

To produce our guide, we asked our online community of more 150,000 government professionals about their cybersecurity challenges and concerns. In this report you'll find answers to 12 cybersecurity questions:

1. What does it mean to be secure? (pg. 9)
2. I am not a cyber professional — why should I care about cybersecurity? (pg. 10)
3. How do we recruit and retain the next generation of cyber professionals? (pg. 11)
4. What strategies can we use to combat insider threats? (pg. 14)
5. How can we create a culture of cyber awareness at our agency? (pg. 15)
6. How can my agency use the NIST Cybersecurity Framework? (pg. 16)
7. What kinds of attacks are we most vulnerable to? (pg. 17)
8. What is our plan when we are attacked? (pg. 20)
9. How can automation help us become more efficient at combating cyberattacks? (pg. 21)
10. What do I need to know about cybersecurity and the Internet of Things? (pg. 24)
11. What's critical infrastructure? Why is it at risk? (pg. 25)
12. What do I need to know about the Continuous Diagnostics and Mitigation program? (pg. 25)

We also interviewed industry leaders to help us further explore the challenges and understand the technical solutions available to the government community. But we know that cybersecurity is a vast, complex field. In this report we hope to:

- Educate government employees concerned about cybersecurity, even if they do not directly deal with cyber issues on a daily basis.
- Improve how IT leaders communicate cyber issues across teams and departments.
- Provide cybersecurity analysts on the frontlines a broad overview of market trends and additional access to cyber resources.

Cybersecurity is not just important to the IT professional; it takes a culture of cybersecurity and awareness to protect data. To protect information today, we must think beyond technical specifications and solutions. Our guide will challenge you to think about how to start a meaningful cybersecurity conversation at your agency.

CONTENTS

Experian®
Public Sector

The power to stay one step ahead of fraudsters

Comprehensive data verification and ongoing validation to help authenticate identities

right decisions } successful missions

Visit experian.com/publicsector or call **1 888 314 8501** to learn more.

CYBERSECURITY IS ABOUT CONTEXT, NOT JUST PEOPLE

User authentication is an integral component of any cybersecurity process. Creating an environment safeguarded from fraudsters, hackers and even misguided internal users requires a robust identity management system. In an interview with GovLoop, Vice President of Strategic Alliances and Business Development at Experian Public Sector, Philippe de Raet discussed how Experian approaches authentication in a way that focuses on the context of access, rather than just the person trying to log on.

He suggested focusing on the specific transaction occurring between the user and an agency to determine the appropriate verification processes. Rather than deploying a cumbersome verification process, agencies should focus on securing the processes most susceptible to fraud while making less sensitive processes more practical and easier to execute.

The reason behind this approach is twofold. Firstly, the burden on agencies to safeguard every virtual process with a cybersecurity system, which may be overkill and counterproductive for employees, is reduced. Lengthy authentication processes can be costly and cumbersome, especially for information that isn't sensitive enough to require heavy credentialing for access.

Over-credentialing can even put your organization at greater risk for a leak by increasing the amount of authentication information you keep on file. "We only release data that's appropriate with the level of assurance needed. Otherwise, you're opening yourself up to fraud by releasing attributes about yourself that may not be relevant for a certain transaction," said de Raet.

Secondly, creating a context-specific identity management system also ensures that security is maintained without impeding employees or external users from accessing necessary information. "The issue around privacy is maintaining that balance between making it practical for the person, yet at the same time secure for the transaction," said de Raet. "People will only adopt what's practical, no matter the risks."

Focusing on the context of a login can ensure you find that balance between privacy and practicality. The goal of the transaction can be a key determinant in deciding what sort of verification is required, and also what the user may be willing to offer in exchange for access. As an example, de Raet explained: "People aren't willing to be frisked for a cup of coffee, but they might agree to offer information about themselves, such as their first name. That said, they might be willing to get frisked to get on a plane, especially if it's the only way to get from one place to another."

Another aspect to consider is *how* the person is attempting to access your system. Instead of focusing solely on information provided at login, adding device intelligence to the authentication process can create a more holistic view of user actions. Experian considers parameters such as typing speed, browsing history, and login location. Thus, even if credentials are correct, the identity management system will know whether the user's account might have been hacked.

Similarly, the device a person uses to log on can add a layer of contextual verification. Increasingly, users are using personal devices to access information. These devices then become a part of that person's identity, and can provide context for a questionable authentication process. As de Raet explained, "Using device intelligence as part of the authentication process is a phenomenal way to close the loop. Even if someone's identity is in question, if we can validate the device being used as belonging to that specific user, we can verify that identity."

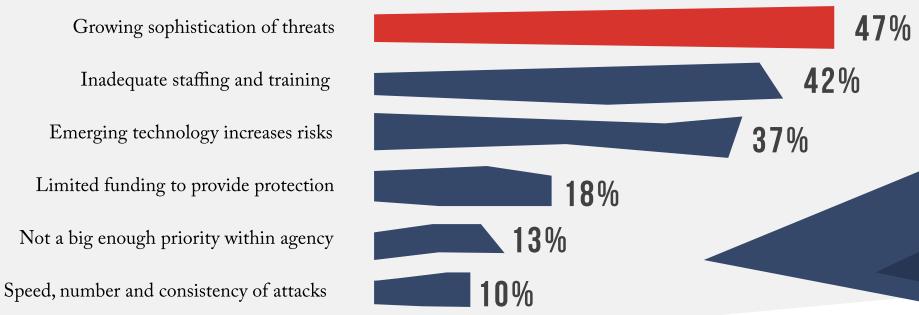
Finally, the verification process must consider the context of the relationship formed by the user and your services. "A straightforward ID proofing session for someone may be well and fine today," de Raet said, "but the context there may not be the same in a month, a year or two years from now." Target threats by studying the habits of individual users over time, and adjusting your safeguards to changes in their behavior. For instance, a user may suddenly access substantially more information than usual without an apparent business need. Your cyberteam can use this as a tip that better security is needed to authenticate that user and his intentions.

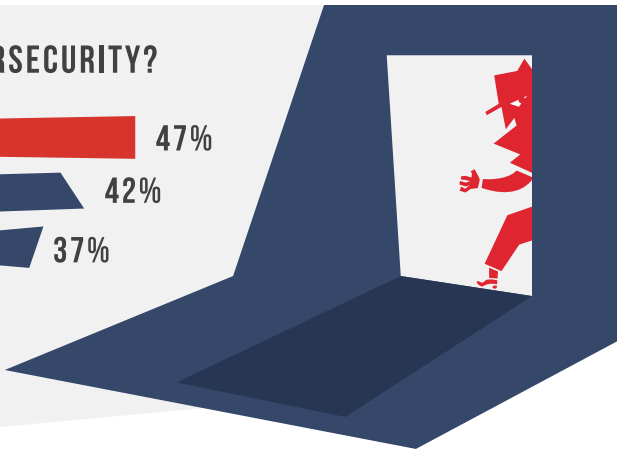
"On the one hand, you want to stay outside of the pages of *The Washington Post.* On the other hand, you don't want to make it so stringent that it's impractical and that people are complaining because they can't get to a website. That balance has to be maintained between adoptability of the offering and, at the same time, the security of that offering," de Raet concluded. Focusing on the context of each access point is crucial to identifying this balance.

THE STATE OF CYBERSECURITY

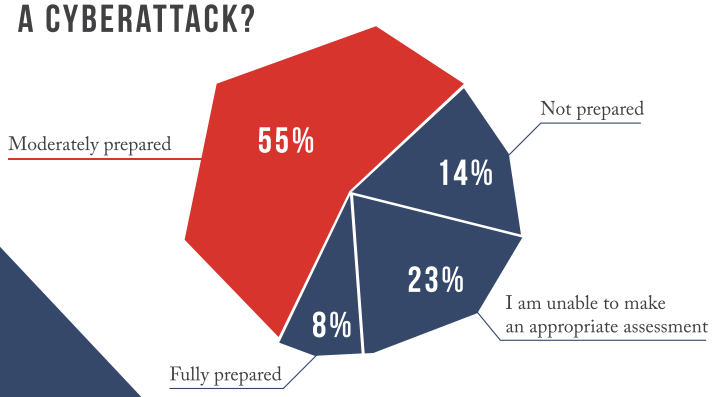
In our survey of 81 members of the GovLoop community, we not only solicited feedback about their biggest challenges, we also wanted to gain a better understanding of the cybersecurity landscape.

WHAT IS YOUR BIGGEST CHALLENGE WITH CYBERSECURITY?

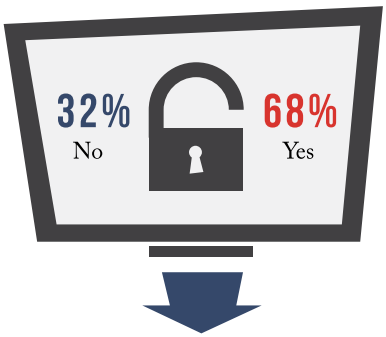




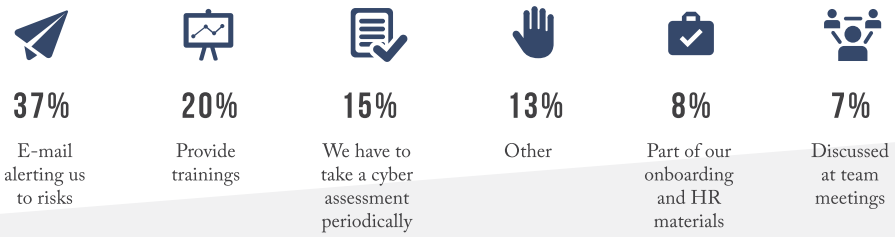
HOW WOULD YOU RANK YOUR AGENCY'S LEVEL OF PREPAREDNESS TO THWART A CYBERATTACK?



DO YOU BELIEVE THAT YOUR ORGANIZATION PROMOTES A CULTURE OF CYBER AWARENESS?



IF YES: HOW SO?



WHAT ARE YOUR CYBERSECURITY BEST PRACTICES?

"Ensure their ongoing training to maintain expertise."

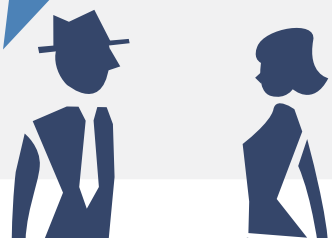
"Constant awareness through testing, sometimes tricky testing but with appropriate consequences."

"Follow or consult a trusted framework (SANS, NIST, etc.), secure the human."

"Never believe you are an expert. This is way you are open to new techniques,"

"Be on the alert at all times."

"Stay educated on latest threats and most up-to-date products offering protection; educate end users."



FireEye
SECURITY REIMAGINED

THE BLINK OF AN EYE

That's how long it takes cybercriminals to bypass most security defenses.

Why do the top retail, financial services, energy, and government organizations trust us to protect them from cyber attacks?

We don't blink.

Scan the code and let us help you close the hole in your network.

carahsoft.

877-9-NO-MALW

www.carahsoft.com/fireeye

© 2014 FireEye, Inc. All rights reserved. FireEye is a trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners.

* Based on FireEye customer engagements

EMPOWERING AGENCY ANALYSTS TO MINIMIZE RISKS

As public information is increasingly digitized, cyberthreats and breaches have the potential to cause catastrophic damage. As society has become increasingly reliant on digital communications and transactions, protecting citizen data from data breaches, intrusions or insider threats is now of the most paramount concern.

With this in mind, cybersecurity mandates and security compliance has become a top priority for public agencies. For a more in-depth perspective, we spoke with Travis Rosiek, Chief Solution Strategist for Global Government at FireEye.

Rosiek notes that compliance to cyber regulations and norms is not enough. "What I've seen in my experience is compliance doesn't mean secure," said Rosiek. He states it is more important for agencies to focus on security, such as detecting and minimizing the threat and impact of cyber attacks. Compliance should be a result of these efforts, but not the sole objective.

When it comes to helping organizations remain secure, FireEye protects agencies from cyber threats with its custom-built security platforms that are specifically designed for real-time malware analysis. "[The Multi-Vector Virtual Execution (MVX) engine] is designed with such high-performance and efficacy that we can actually generate intelligence on premise that can be used to minimize the impact of a current threat without user interaction," explains Rosiek.

FireEye helps minimize risks by empowering agency analysts and security teams, giving them actionable information with rich context around suspicious activity. With the sophistication of the next generation of cyber attacks, the automatic execution of pre-approved security measures helps improve consistency and early detection. This is especially important given that a 2013 Mandiant report found the median time from an organization data breach to detection was 229 days. What's more, 67 percent of these organizations only learned of the breach via third party notifications and 100% had Antivirus up to date.

Additionally, it is critical for organizations to stay current on the latest cybersecurity strategies, advises Rosiek. Agencies need to promote continual learning and be aware of new vulnerabilities. Employee training and a sound security infrastructure are crucial to this effort.

"By understanding the capabilities of your adversaries you can better posture yourself – whether it be personally for training (i.e. how attacks works) or for your organization's security infrastructure – and this will mitigate some threats," says Rosiek.

And it doesn't matter if you're not a high-profile organization or in an IT-related field. "Most people don't think that their information is important," Rosiek notes. "But to an adversary or competition or somebody else, it's invaluable." Since cybersecurity programs impact everyone, it is important to clearly communicate with all employees, provide relevant context, and avoid intimidating technical jargon.

On an everyday basis, organizations face the daunting task of protecting their information networks. Given Rosiek's experience working with public sector organizations, he provided what he views as the top five current cyber challenges:

1. **Acquisition models** – The majority of the public sector's IT/cyber defense acquisition models are lacking. The adoption of technology including cloud and mobile applications are creating new concerns regarding privacy and security. Keeping up with this rapidly evolving landscape can prove to be a significant task.
2. **Cyber Workforce** – Low retention rates and shortages of the cyber workforce in the U.S. impede progress towards sustainable and secure organizations. To address this concern, FireEye launched initiatives with STEM students, aiming to get young people more interested in this high-demand field.
3. **Cyber Legislation** – Contention on the Hill regarding cyber security laws slows down or prevents progress. For the legislation that is out there, there are often significant gaps in the policy or implementation.
4. **Legal Constraints** – Globally Cyber defenders have many legal constraints they must navigate. "Adversaries know what these legal constraints are and they use them to their advantage," says Rosiek.
5. **Cyber Mindset** – The importance of being compliant versus being thoroughly secure. Organizations should understand that it is essentially inevitable that they will be breached at some point. Thus, preparation and planning are critical to reduce cyber risks and minimize potential damage.

Although these are the challenges that agencies face today, it's important to remember that the threat landscape is constantly changing and evolving. As tools grow in sophistication, so do the threats facing agencies. Due to this, organizations must be sure they have created a culture of cybersecurity, and staying current with the latest threat detection and mitigation strategies.

Today, public agencies must navigate a digital landscape full of increasingly complex cyber threats. However, with better awareness and training, and the help of cybersecurity vendors like FireEye, such challenges can be faced with confidence.

YOUR TOP CYBERSECURITY QUESTIONS ANSWERED

We solicited feedback from the GovLoop community about the most pressing questions about cybersecurity. Here are the 12 top questions and our answers. We love feedback, so if there's a question we missed or you want more information, send us a note at info@govloop.com.

QUESTION #1: WHAT DOES IT MEAN TO BE SECURE?

Maintaining and protecting valuable assets are two of government's most important tasks. Your agency may very well hold crucial information about our economy, confidential citizen data or national security intelligence that must remain protected. The stakes for data security are higher than ever before. So how can administrators confidently say their data is secure?

At its surface, this question seems simple. Administrators can point to technical specifications they follow, network assessments and tests, staff security trainings, and more.

Yet in reality, the question is so fundamental, it deserves more attention than checking off a simple list of procedures. Our question is humbling in its complexity and indicates that security today is not just a physical state; it is a mind-set that must diffuse across an entire agency.

One of the major challenges you face as a government employee is closing the gap between your perceived and actual security. By fully assessing your security levels and closing that gap, you can stay one step ahead of attackers and protect your agency's data.

Here are five core competencies you need to be secure:

1. The ability to gain real-time awareness of networks.

Attacks on agencies are occurring more frequently than ever before, and agencies now must be able to analyze threats and attacks in real time. Being secure doesn't just mean the ability to respond quickly; it's having the knowledge and insights to spot attacks as they are unfolding. To gain that awareness, agencies must understand what their network looks like, who accesses it and how.

2. Create ways to continuously conduct vulnerability assessments.

In today's security environment, organizations must respond quickly to an attack. Your agency must be able to deploy mitigation techniques and respond rapidly to complex attacks.

3. Educate and train employees.

Cyber professionals must be able to communicate the importance to employees outside cyber- or IT-focused departments. Be creative with training and educating your employees — an area we explore more later in our report.

4. Assess your network.

How can you protect your network if you don't know who or what is on it accessing information? The ability to continuously assess your network is imperative. This means conducting data inventories, and most importantly, understanding how information moves across your network.

5. Automate processes.

Automation is a crucial part of any cyber defense. By automating traditionally manual processes, agencies can improve compliance and reporting strategies. Automation can help agencies react quickly and develop new ways of thinking about cyber issues.

Ultimately, the problem that security professionals face is that some attacks will work. Cybersecurity today is as much a practice of damage control as it is of prevention. These five competencies are by no means exhaustive, but they are fundamental to any cybersecurity strategy.

As we progress through our report, keep these competencies in mind and map them back to your agency. Defining security in a modern context is difficult, but with hard work and holistic thinking, you can take important steps to improve your overall security posture.

QUESTION #2: I AM NOT A CYBER PROFESSIONAL – WHY SHOULD I CARE ABOUT CYBERSECURITY?

Since the Clinton administration, the United States' interest in cybersecurity has increased exponentially. Due to the influx of new technological advancements, government has faced the challenge of modernizing IT and preserving systems' security. Throughout his administration, President Obama has emphasized the importance of cybersecurity, classifying cyber as one of the greatest national security and economic threats to our country. At the same time, America's economic growth in this century depends on cybersecurity, he said. We are operating in an unprecedented globally networked era, and as such, cybersecurity has become extremely important to IT professionals. But for other workers, why does cyber matter?

Government contractors are particularly susceptible to cyberattacks because the U.S. government is the largest producer, collector and disseminator of data in the world. To combat these threats, the Defense Department now requires private contractors to fulfill strict safeguarding measures in addition to their previous task of protecting classified data. Startup contracting firms are the most vulnerable to cyberattacks because of the high cost of complying with these cybersecurity requirements, said Geoff Orazem, president of a Washington, D.C.-based incubator for federal contractors called Eastern Foundry.

Cybersecurity significantly affects contracting firms because they face greater commercial and legal risks relative to other businesses. Furthermore, contractors have to decipher each agency's inconsistent standards and rules and the often-vague compliance requirements of the federal government. Failure to adhere to these unclear requirements leads to more severe penalties than other companies face. Examples include the government withholding payment or terminating a contract by default. At worst, the government can suspend companies from performing all future contracts as a penalty for cybersecurity compliance problems. Finally, a government contractor that fails government-mandated cybersecurity protocol can be forced out of the industry entirely.

For non-IT professionals under oath to protect the confidentiality of their clients, this is especially important. For example, legal professionals need better training on how to deal with cybersecurity threats and should be particularly aware of corporate security breaches, said Ralph Losey, an attorney and founder of e-Discovery Team LLP. When hackers can't directly access a company's data, one method they use is attacking corporate lawyers who have access to massive amounts of the company's data. Therefore, it's vital for attorneys to be aware of their vulnerabilities and take cybersecurity training courses to better prepare for these types of attacks.

QUESTION #3: HOW DO WE RECRUIT & RETAIN THE NEXT GENERATION OF CYBER PROFESSIONALS?

The public sector is constantly protecting itself against hackers and online security challenges. With a lack of skilled talent in the cybersecurity workforce, the federal government is especially susceptible to falling victim to cyber attacks.

Agencies desperately need to hire skilled cybersecurity professionals, but are enough properly trained professionals in the market? How can government compete against the private sector, which can pay better salaries and offer more benefits? How can government make sure it's investing in the proper workforce training for existing employees? These are essential questions that agencies must consider, especially as a new generation of cyber professionals enters the workforce.

The Bureau of Labor Statistics forecasted that between 2012 and 2022 the labor force will add more than 27,000 information security analyst jobs. But a June 2013 Government Accountability Office report shows a 22 percent vacancy rate in the Homeland Security Department's (DHS) Cyber Security Division. Where will these workers come from?

When Ira Hobbs was the chief information officer at the Treasury Department, he made cybersecurity hiring and training top priorities.

"We need to be able to harness [cyber] talent so it works collaboratively and is integrated across very large departments with very different informational requirement needs," he said in an interview with GovLoop. "Then once you acquire the talent, then, how do you keep them trained and ready so they can keep responding to new threats that continue to arise daily?"

The federal government has long been aware of the cyber workforce problem. In early 2010, NIST became the lead agency for the National Initiative for Cybersecurity Education (NICE), created explicitly to deal with federal cybersecurity professional development. NICE worked to create workforce structures to grow talent within government and provide additional training and professional development opportunities.

"The National Institute of Standards and Technology (NIST) is leading the NICE initiative working from the strengths and energy of more than 20 federal departments and agencies, to ensure coordination, cooperation, focus, public engagement, technology transfer and sustainability," according to NICE's website.

But attracting and retaining talented cybersecurity professionals is still a serious challenge for the government. According to a recent study, H4cker5 Wanted: An Examination of the Cybersecurity Labor Market, produced by the Rand Corp. in June 2014, the shortage of cybersecurity professionals is largely an issue of hiring people at the top level — the best of the best.

"These are the people capable of detecting the presence of advanced persistent threats, or, conversely, finding the hidden vulnerabilities in software and systems that allow advanced persistent threats to take hold of targeted systems," the report states.

To attract them, the report suggests:

Recruit early. One strategy is for agencies to continue to engage with the hacker community and create robust recruitment strategies. Rand's report recommends starting recruiting at the high school level and providing collegiate scholarships for cyber-related programs.

Differentiate job categories more precisely. In job descriptions, human resources managers should be sure that the various subspecialties in cybersecurity are clearly stated. This will attract better candidates, and skilled applicants can be more quickly identified, recruited and hired.

Address civil service issues, particularly salary. "Salaries that top out at $150,000 are uncompetitive for those who could otherwise command twice as much," the Rand report states. It also notes that the federal government faces constraints in being flexible around matching salaries. If these issues could be resolved, the report suggests, the hiring and recruitment of cybersecurity experts to the government would be a much easier prospect.

Many organizations, such as the National Science Foundation (NSF), are taking these recommendations to heart. NSF will fund 10,000 computer science classes in public high schools by 2016. Two pilot courses, introductory "Exploring Computer Science" and a more advanced "Computer Science Principles," are being financed through NSF grants, according to a report in The Washington Post.

Want to attract and retain more cybersecurity experts? You can follow the National Security Agency's model, the Rand report states. "Fewer than 1 percent of [NSA] positions are vacant for any length of time, and supervisors report being very happy with the personnel they get. NSA also has a low turnover rate. One reason is that it pays attention to senior technical development programs to ensure that employees stay current and engaged."

"Our interview suggests that the NSA makes rather than buys cybersecurity professionals," the Rand report adds. Eighty percent of NSA's new hires are entry-level employees with bachelor's degrees, and the agency has developed one of the best intensive training programs in the country.

You may not be able to effect changes in cybersecurity hiring, but changes to general HR and hiring practices can have an effect on the level of expertise your agency is able to attract overall. GAO's recommendations on creating and implementing a strategic workplace plan are valuable in this regard; you can read them in this report.

More resources:

- H4CKER5 WANTED: An Examination of the Cybersecurity Labor Market
- Cyber In-Security: Strengthening the Federal Cybersecurity Workforce
- Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination


If you want better security, think like a bad guy.
It's only a matter of time. Bad guys will get into any network sooner or later. They may already be inside. HP Enterprise Security Products has the cybersecurity technologies your agency needs to prevent, detect and stop adversaries before any damage is done. Our continuous monitoring enterprise security products give you real time response, a full range of capabilities, and are easy to deploy and maintain. HP's integrated platform documents all events, continually refining and improving protection. Your vital agency systems stay protected while delivering services safely and efficiently.
Better security. See how it strengthens your mission. Visit hp.com/go/fedsecurity
Make it matter.
carahsoft.
Follow us on Twitter @HPGovSec
Platinum Partner with Carahsoft
888-55-HPGOV | www.governmentITplaybook.com
© 2014 Hewlett-Packard Development Company, L.P.

BALANCING RISK AGAINST INNOVATION

In today's technologically inundated world, cybersecurity is an issue that affects public and private sectors alike. GovLoop recently had the opportunity to speak with Rob Roy, the federal chief technology officer at HP Enterprise Security Products on these issues. Roy provided valuable insights on the most pressing cyberthreats, the best security practices for both IT and non-IT professionals, and ways in which HP is helping the public sector.

When highlighting today's major cybersecurity threats, Roy took a holistic, macro-level approach. He mentioned that agencies face both external and internal threats when it comes to protecting information networks. On the one hand, organizations are faced with advanced persistent threats from hackers, nation states and other malicious actors on a near-daily basis. However, it's not enough to protect critical agency data from outside threats alone. Roy says the challenges presented by insider threats and other individuals looking to expose sensitive organizational data must be met with equal vigilance.

According to Roy, insider threats are not necessarily malicious. He acknowledged that federal agencies are also vulnerable to accidental information breaches, which can be avoided with greater security training and threat intelligence.

In terms of best practices, Roy emphasized the importance of limited access. "Everything runs on software, and it is designed to allow people to access the network," Roy said. "The key is that it has to ensure that access is limited to only those who have permission. Organizations need to look at the software layer, from acquisition to development and production, assuring the software supply chain from intentional and unintentional vulnerabilities."

Roy also cited the importance of deploying continuous monitoring solutions. One such example is HP's work with the Department of Homeland Security and its Continuous Diagnostics and Mitigation (CDM) program. The program is a government-wide purchase agreement that can be used by any local, state or federal government agency to procure a wide array of continuous monitoring services and tools intended to improve the cybersecurity posture of the government. Through the CDM program, HP helps DHS provide government organizations and employees with tools designed to identify risks on a continuous basis.

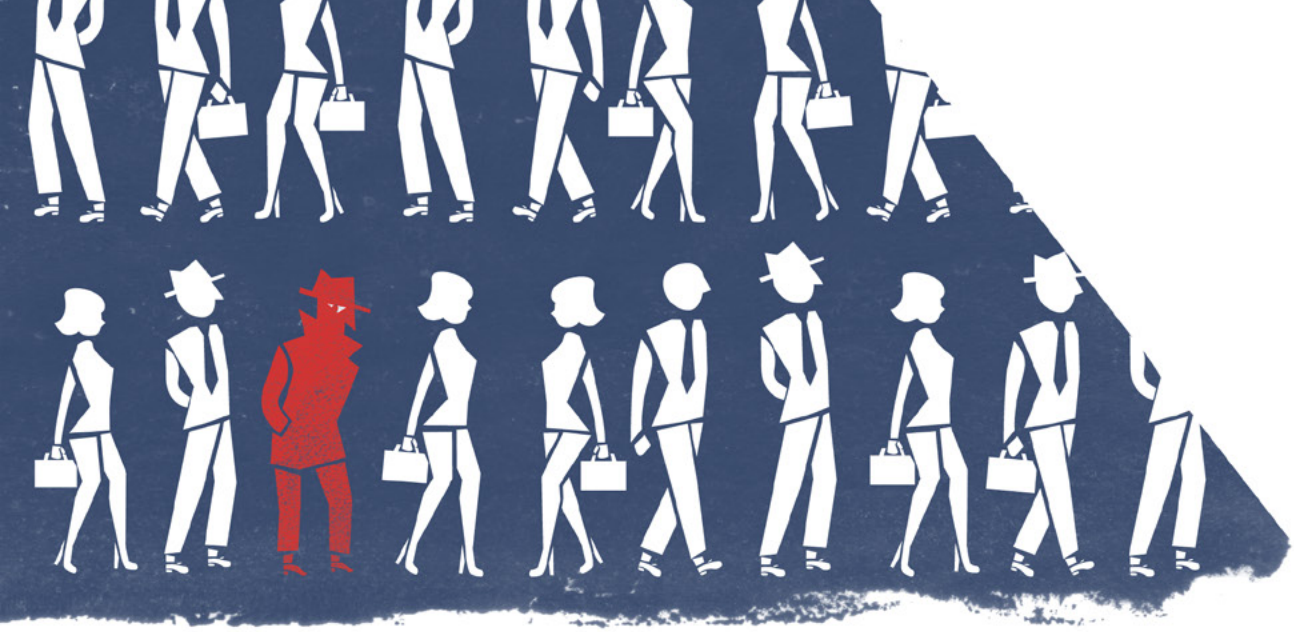
But HP did not just stop at the development, production and sale of the CDM program. The company broke down the entire concept of CDM and began training federal employees through marketing actions and individual HP sales personnel. HP hosts weekly trainings not only on HP technologies but also on valuable information such as developing secure software applications. As part of this more proactive approach to the cybersecurity challenge, HP is able to get the necessary information out to the public in an easily consumable manner.

"CDM consists of 15 discrete but highly powerful security control areas, and we broke that down into four main areas that all 15 controls fit into," Roy explained. "There is configuration management, understanding what you have to protect, vulnerability management, understanding where the risks are, access management, which includes who has access and how do we control what they access, and finally event management, which includes how we discover when we are being attacked and how to we respond effectively."

HP also helps public sector agencies remain secure in a numbers of other ways. HP Security Research (HPSR) is a global, independent security research group that delivers security intelligence and vulnerability research to its customers. HPSR assists HP's government customers in managing their data responsibly and securely. As part of its new developments, HP's data security and cryptography vendor Atalla is now offering cloud encryption that combines patented, key-based encryption technology that increases security through measures such as protecting keys when they are in use in the cloud. HP intends to converge its different security ideas and technologies in order for people to help each other tackle cybersecurity threats.

So, how do we balance cybersecurity practices with innovation? "In general, innovation introduces risk, but it should not prevent us from innovating," Roy said. "For balancing the risk, look at the software and the network; see if a piece of hardware is coming from a legitimate original equipment manufacturer; and look at the supply chain for the innovation and whether or not it has the supply chain risk management assurances built in."

Despite the growing number of IT threats, technological innovation can proceed in a secure manner. By taking a proactive approach to cybersecurity initiatives, organizations can stay one step ahead of attackers, and protect the confidential data they store and manage.



QUESTION #4: WHAT STRATEGIES CAN WE USE TO COMBAT INSIDER THREATS?

Insider threats can have severe consequences, with victim organizations facing significant costs and damages. According to the FBI, the average cost per incident is $412,000, with victims losing an average of $15 million a year. Although most agencies primarily focus on external cyberthreats, it is crucial to also prepare and combat insider threats.

The U.S. Computer Emergency Response Team (CERT) defines an insider threat as:

> *A current or former employee, contractor, or other business partner who has or had authorized 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 are not necessarily hackers and they often don't start with malicious intent. Usually a trigger event — such as a denied vacation or being bypassed for a raise or promotion — initiates the threat. What's more striking, the CERT Division of the Software Engineering Institute (SEI) at Carnegie Mellon University found that 90 percent of IT saboteurs were system administrators. Despite this, most security tools are designed with hackers in mind, but they're not always the real threat.

For a more overarching, office-wide approach, Patrick Reidy, former chief information security officer at the FBI, offers three pieces of advice regarding insider threats:

- A good insider threat program should focus on deterrence, not detection. An employee's work environment, regardless of job function, should discourage insiders by crowdsourcing security and deploying data-centric, not system-centric, security. By creating a data-centric approach, organizations can monitor how data moves across an agency and block certain actions from occurring. This gives a more holistic view of data, rather than just simply monitoring a workstation or specific network systems. This helps create an environment where it is difficult to become an "insider."
- Avoid the data overload problem. In security efforts, do not get overwhelmed with data. Reidy proposes that only two sources of data are needed: HR data to better understand employees and workplace or personnel issues and system logs to track what is being printed or downloaded via USB, CD or DVD.
- Detection of insider threats must use behavior-based techniques. Detecting insider threats is very hard, like looking for "a needle in a stack of needles," Reidy said. By using behavioral analytics, agencies can build a baseline of behavior and look for red flags — anomalies that differentiate potential insiders from innocuous employees.

The CERT Division of SEI also provides 10 best practices to prevent and combat insider threats:

1. Institute periodic enterprise-wide risk assessments and security awareness training for all employees
2. Implement strict password and account management policies and practices.
3. Log, monitor and audit employee online actions, especially unusually large queries, downloads, print jobs or e-mails, or other suspicious behavior.
4. Use extra caution with system administrators and privileged users
5. Collect and save data for use in investigations.
6. Implement secure backup and recovery processes.
7. Clearly document insider threat controls.
8. Provide an Employee Assistance Program or other recourse for employees experiencing personal problems.
9. Deactivate computer access and change passwords for all accounts upon termination, including external accounts.
10. Train management on the patterns of behavior that could indicate an IT sabotage attack.

Insider threats present potentially catastrophic risks for all organizations, no matter what sector. But preparation, awareness, training, periodic assessments and the implementation of security measures and strategies can decrease an organization's vulnerability.

QUESTION #5: HOW CAN WE CREATE A CULTURE OF CYBER AWARENESS AT OUR AGENCY?

For an organization to remain secure and effective, its workforce needs to be cyber aware. Simply put, cyberattackers don't discriminate. They will target any organization, regardless of its cybersecurity readiness efforts. Therefore, the first step in creating a culture of cyber awareness is to understand that every part of and every employee at your agency is a target. This observation is not meant to frighten or intimidate. Instead, it is a call for officials to recognize and meet their obligations, especially those at public agencies that hold massive amounts of sensitive data.

Whether employees know it or not, they play an integral role in their organization's cybersecurity. If not already in place, mandatory periodic security training for all employees is a great way to spread and maintain awareness. It is also critical to train managers on a range of cybersecurity issues such as social networking and the communication of sensitive data, in addition to making them aware of common cyber threats and patterns of behavior — both external and internal — that could indicate an attack.

In today's digital, data-driven age, cyber awareness should be a basic requirement for public agencies. No one expects to be the target of an attack, but that doesn't mean it cannot or will not happen. This realization and the duty to protect the interests of the public can go far to promote a culture of cyber awareness at public agencies.

QUESTION #6: HOW CAN MY AGENCY USE THE NIST CYBERSECURITY FRAMEWORK?

In accordance with Executive Order 13636, Improving Critical Infrastructure Cybersecurity, NIST released a framework in February 2014. The framework is the result of collaboration between industry and government leaders to identify, analyze, and consolidate standards and practices for cyber risk. The resultant strategy provides a way to tackle threats to cybersecurity, while protecting citizens' privacy and civil liberties. It is not meant to replace any existing policies or regulations. Instead, it creates a new, standardized and holistic framework to assess and address your organization's susceptibility to cyberattacks.

Compliance with the framework is voluntary, but that doesn't mean it isn't applicable to your agency. NIST recognizes that there is no one-size-fits-all model for managing risk. In fact, the agency created the framework to be adaptable to any sector, technology infrastructure or risk environment.

Instead of creating a single template for everyone to follow, the framework provides four tiers against which to analyze your risk management strategy profile. These range from Partial (Tier 1) to Adaptive (Tier 4) and should be adopted to fit your agency's specific needs and capacity. In addition, the framework covers 16 infrastructure sectors, including communications, energy and government facilities, to ensure that it is applicable to every mission. No matter what your agency does, the framework can help you identify, hone and improve your cyber risk strategy

Using the framework should not be a one-time effort. This is an ongoing process of scrutiny, comparison and revision that will take time and will likely be repeated as advances are made in each aspect of your risk management strategy. Just as the cyber environment evolves, your risk tolerance, susceptibility and management capacity will also evolve. Therefore, the framework's processes should become part of your agency's everyday practices to make sure that, as new threats arise, your agency is ready with the tools to address them.

You can get started by learning and applying the basics of the NIST Framework. Arguably its greatest benefit is a set of standardized definitions for the five main functions of cyber risk management: Identify, Protect, Detect, Respond and Recover. Each of these Framework Core elements is further detailed within categories and subcategories, and references current industry practices. Use these terms, definitions and their respective components to get everyone, including agency employees and external stakeholders, on the same page about cybersecurity risk. Then, narrow your scope.

Your agency will need to tackle risk across the board, but that doesn't mean it has to be done all at once. Start by identifying the priorities, systems and assets of a single process. Finally, use the Core elements to assess your current risk susceptibility and tolerance within that process. The framework emphasizes that before you can improve your cybersecurity, you first have to determine where you are and whether you're meeting your agency's needs. If you find that you're at greater risk than you should be, it's time to dive into the framework's processes of assessment, targeting and improvement.

QUESTION #7: WHAT KINDS OF ATTACKS ARE WE MOST VULNERABLE TO?

When you hear "hacker" or "security breach," you might envision a masked culprit haunting your computer system, but this isn't always the case. To avoid potential cybersecurity breaches, it's important to know where your agency is most vulnerable.

As our report has outlined, many of the risks associated with cyber often stem from a lack of employee awareness. In a Forrester Research report, Understand the State of Data Security and Privacy, an employee survey revealed that one out of four respondents thought security breaches were a result of a disgruntled employee, but 36 percent of data breaches were due to employee errors and carelessness with data handling. Businesses continue to increase spending on antivirus software and other tools to fight hacking, but many of the problems stem from careless or fraudulent employee behavior.

Aside from developing and mandating more efficient cybersecurity training for employees, it's necessary for organizations to be aware of how they handle data. Before making a plan of attack against cyber criminals, it is important to analyze and inventory your data to determine potential vulnerabilities.

First, a company has to determine what types of data it handles and what is more sensitive and valuable. Create a ranking scale to identify data's levels of value and develop level-specific security measures. Second, an organization should determine its data processing procedure: which data is at rest, held in persistent storage, and which is in transit, or processed by a central processing unit such as the hardware within a computer that carries out the system's basic logical and arithmetic functions. The more data is moved from one computer to another, the greater the potential for a security breach. Third, an agency needs to identify who is accessing the data and under what circumstances. Company data shouldn't be accessible to all employees. For example, a marketing team does not need access to employee payroll information.

According to Norton Symantec, here are the top 11 threats to watch for:

1. Virus: A piece of software that can replicate itself and infect a computer. Viruses can only be transmitted via a network user, the Internet or through removable software.
2. Spam, Spim, Spit: Spam is electronic junk e-mail. Spim is spam sent through instant messaging systems (i.e., Yahoo!). Spit is spam sent via Internet telephony and comes in the form of unwanted, auto-dialed phone calls using voiceover software.
3. Pharming, Phishing and Spoofing: Pharming occurs when a hacker redirects a website's user traffic to a different, fake site. Phishing occurs when a bogus page appears in place of a legitimate website. Spoofing is a cyberattack in which a program or person impersonates another.
4. Spyware: Software that is secretly installed on a computer without the user's consent.
5. Keystroke logging: A keylogger is a software program that is installed on a computer, usually by a virus or a Trojan horse, and it records users' keystrokes.
6. Adware: Software that automatically displays, downloads or plays advertisements on a computer.
7. Botnet: A group of software robots (known as bots) that run automated tasks on the Internet.
8. Worm: A self-replicating, malicious software program. Unlike a virus, it doesn't require attachment to an existing program in order for it to infect a system.
9. Trojan Horse: Software that conceals a usually malicious payload while seeming to execute a legitimate task.
10. Blended threat: Combines different malicious elements, such as a Trojan and a virus, and uses many techniques to spread itself.
11. Denial-of-Service Attack (DoS): A method to make computer resources (i.e., a web server or a website) inaccessible to users. The most common DoS attack is flooding the target machine with external communications requests, which makes the machine unable to respond to legitimate user requests and traffic.

Remember, the first step to enabling better cybersecurity practices is through greater knowledge of potential threats.


HYTRUST®
Cloud Under Control
Is your agency safe from insider threats?
HyTrust Virtualization & Cloud Security helps agencies operate securely in private or public clouds and protects against insider threat with:
Administrative Controls
Continuous Monitoring and Alerting
Encryption and Key Management
Automated Compliance
Two-Man Rule
HyTrust solutions are available through
carahsoft.
Learn more at InsiderThreatReport.com

WHY YOU MUST CONSIDER POLICY-BASED CONTROLS AND ROLE-BASED MONITORING FOR CYBER DEFENSE

In a rapidly expanding cyber landscape, agencies must ensure they have deployed the right IT solutions to spot common abnormalities, automate alerts and conduct role-based monitoring to proactively stop attacks and protect information.

"Government has definitely been talking about cybersecurity and cyberattacks as the next battle ground for the last few years," said Eric Chiu, president and founder of HyTrust, in an interview with GovLoop. But the problem for many is that intruders are already inside the network, and the stakes are higher than ever before.

To prevent attacks, organizations are aggressively seeking solutions to improve the visibility and control of internal networks. This means understanding how data moves across networks and securing cloud environments, while providing the proper access to information that empower decision makers.

At HyTrust, the company is looking at ways to ensure security, compliance and availability. One way it does this is by enforcing policy over every action that is attempted in a cloud environment. For instance, if an administrator should not be permitted to copy or delete virtual machines, they should be restricted from those capabilities. If they skirt around security protocols, the action should be denied and other administrators should be alerted of the unwarranted access. Chiu also noted that for sensitive operations, organizations should consider implementing the "two-man rule," which requires a second person to authorize sensitive or dangerous operations like copying or deleting virtual machines with sensitive or critical data.

"A lot of people talk about continuous monitoring and it's a great initiative. However, you need to monitor the right activities, and the world is moving past the traditional perimeter-based security approach," said Chiu.

With more people using the cloud and mobile devices, the idea of having a "perimeter" in which your data is neatly stored and hosted, has disappeared. With changes to how data flows across networks, public sector organizations need to take a new approach.

This is why role-based monitoring is so important. "Role-based monitoring means that you are monitoring specific actions of users and administrators within your environment, especially when they are managing systems that house sensitive data," said Chiu. "You can then compare what they are doing versus what their role is, what they should be doing, and what they typically do in your environment. Once you gain this kind of awareness, you can recognize when things are essentially out of place."

If an attempt is made to access data, the only way to know if it is legitimate or not is to be able to monitor actions and compare them to what that individual should be doing on a network. This is why role-based monitoring is an imperative piece to your cyber defense programs.

"We have built-in alerts that not only send email alerts to higher teams of people, which say this activity is happening that looks suspicious and is triggering your alerts, but we can proactively stop the action as well. So let's say this person doesn't have the role to make copies of virtual machines or make copies of classified virtual machines. We can stop the action before it ever happens," said Chiu.

To get started with improving network resilience, Chiu offered a few suggestions that organizations can take to increase security. "In this day and age you have to assume the bad guys are already in your network," said Chiu. "That one simple assumption would dramatically change how agencies secure critical systems and data."

This is because by acknowledging that people are already in their networks seeking to compromise data, cyber officials can start taking proactive steps to minimize impact, and reduce or eliminate the threat. Organizations could then deploy access control, the two man rule, role-based monitoring, or encrypt data for additional security. "Those initiatives come about because you have shifted your thinking, and recognize that perimeter security is no longer adequate," said Chiu.

Another step to take is to be sure to be monitoring the normal course of business for security and compliance purposes. This will help you develop the right controls, and not just monitor activity, but also prevent incidents from occurring.

With emerging technologies and solutions, organizations can have the confidence that they have taken the proper steps to secure their data and networks.

QUESTION #8: WHAT IS OUR PLAN WHEN WE ARE ATTACKED?

Having a strong cyberattack response plan is critical to the security and effectiveness of any organization. Recent data security breaches involving Target, P.F. Chang's, Sally Beauty Supply and most recently The Home Depot have reaffirmed the importance of being prepared for such attacks. The initial response to an attack is crucial, but the preparation and groundwork agencies do beforehand is of equal, if not greater, importance.

To prepare, the New York-based Practical Law Company suggests creating a risk rating to classify reported incidents on a scale of low, medium or high risk. This way, when an incident occurs, the appropriate response can be promptly deployed. Additionally, a compliance work plan should be created — and updated frequently — that includes policies, code of conduct, training and specific incidence response procedures related to cyber risks.

When cybersecurity infrastructure is set in place, the first hope is that it does well enough for the agency to not have to worry about an attack. Simply assuming you're safe, however, is never a good idea. So, should an attack occur, the response team should conduct an initial investigation using a predetermined checklist in the incident response plan to ascertain how serious the attack is. Regardless of severity, however, the response team should always aim to stop the intrusion from spreading and appropriately document the investigation.

This response should be swift, said Gene Quinn, a patent attorney and founder of IPWatchdog. "Pull the plug to stop the attack, identify what from a technical standpoint allowed malicious access, fix the technical glitch, make sure that no latent vulnerabilities exist and improve security before considering going back online," he said.

It is crucial to act swiftly because hackers know they have a limited amount of time to disseminate the information — credit card, medical and other sensitive data — they find, so the quicker the response, the better. Additionally, installing new security software and password protections to prevent similar attacks in the future is a must.

After the response, an internal investigation is important. Practical Law Company notes that an investigation allows an agency to:

- Gain a fuller understanding of the computer intrusion.
- Increase its chances of identifying the attacker.
- Detect previously unknown security vulnerabilities.
- Identify required improvements to computer systems.

Unfortunately, even if your organization does everything right, it is still likely that damage will be inflicted from a successful attack. One example comes from Novice to Advanced Marketing Systems, a provider of marketing training courses and materials, including online seminars. It lost $75,000 in the effort to overhaul its computer systems in response to a malicious attack. "An ounce of prevention is certainly worth at least a pound of cure!" Quinn said.

There are many great resources for CIOs, IT workers and public managers. Some we recommend include:

The Computer Security Incident Handling Guide, published by NIST, which assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively.

The SANS Institute provides information security training and security certification, and research documents about various aspects of information security.

Cyber threats are increasingly pervasive and hackers are becoming more and more sophisticated. And seeing that the Centers for Disease Control and Prevention has a plan for a zombie apocalypse, there's no reason for public agencies to not have a plan in place for cyberattacks.

QUESTION #9: HOW CAN AUTOMATION HELP US BECOME MORE EFFICIENT AT COMBATING CYBERATTACKS?

With more diverse information being stored in a wider variety of methods and mediums, the number of potential threats to cybersecurity increases every day. At the same time, many organizations are forced to cut, or at least maximize the efficiency of, the workforce that combats these attacks. New solutions that automate prevention, detection and resolution of cyber vulnerabilities will have to be implemented if organizations are going to remain secure under mounting threats.

Automation has several benefits. On a basic level, automating cybersecurity processes can save you both time and money by streamlining your cyber defense tactics. This is a necessity as the number of potential threats grows beyond manual capacity to monitor them.

Additionally, automation offers your organization more comprehensive security. It can detect active and latent threats in real time, round-the-clock. What's more, automated cybersecurity can identify a larger variety of threats, because processes to monitor different devices, compliance policies and programs automatically update with the latest threat information.

Finally, automation removes the element of human error that comes with manual cybersecurity monitoring. Navigating an increasingly complex web of vulnerabilities is simply better suited to automated processes.

That doesn't mean that once your agency's cybersecurity is automated, your risk management team will become obsolete. It's still an integral part of your cybersecurity infrastructure. Reducing manual processes diminishes the time IT managers spend monitoring security and increases the time they have to focus on what they were hired to do: combat cyberattacks and develop innovative cybersecurity strategies.

Even as systems monitor the integrity of your network, you still want your team ready to respond quickly when threats do arise. As a recent GovLoop blog post pointed out, even the best cybersecurity organizations can build only so many walls to keep out hackers. Automating routine processes will give personnel the bandwidth to prepare for those instances when attacks do make it through your defenses. It will also give them the tools with which to combat those attacks efficiently. By identifying the location, timing and type of threat, your automated processes will guide IT personnel directly to the source of the attack.

With this information, your team can focus on countering the threat at hand as soon as it emerges, rather than having to check the entire cybersecurity system for inconsistencies.

Even when your team isn't countering breakthrough attacks, automated processes can maximize your workers' productivity by allowing them to focus on the evolution of your cyber strategy and prepare for the future. An effective cybersecurity strategy requires strategists to create complex systems now and adapt them as the risk landscape changes in the future. Automation of basic processes alleviates burdens on time and personnel, so that those resources can be redirected toward strategy development. Given the speed with which new threats arise and morph, you want your IT personnel to be focusing on the evolution of your cyber strategy rather than its maintenance.

As you shift the focus of your cyber strategy, you will likely want to consider restructuring your cybersecurity department and redefining the roles within it. Rather than doing a complete overhaul, you can start by asking your cybersecurity team to think differently about the mission. It will no longer be the first line of defense but a team dedicated to strategically tackling cybersecurity.

At the same time, start looking at the basic processes in your current security infrastructure that could be easily automated. Rather than taking on broad security issues at the outset, think about automating detection of line-item processes that are crucial but small components of your larger security management system. This will get your organization acquainted with automated security and free your staff to start revamping strategy.

Finally, as you start automating processes, make sure that each component assimilates directly into your current workflows and needs. The purpose of automation is to make things more efficient, not add a new level of complexity to your cybersecurity systems.

For more insights into how automation can improve your cybersecurity strategy, take a look at GovLoop's Continuous Diagnostic and Mitigation Program Field Guide. To learn more about how to merge your automated and personnel processes to manage cybersecurity, listen to a recent "DorobekINSIDER" podcast on the topic.

SWISHDATA PRESENTS CYBER ATTACK DEFENDERS: HACKED

HACKED: the series

Federal Agency Employee "PWNED" by Russian Hacker

Watch Hacked, a Cybersode-styled video series, and see how Bob, a federal employee, got caught up in a cyber-situation unbeknownst to him that resulted in dire consequences to his agency, his family and himself.

www.CyberAttackDefenders.com

SwishData
DATA PERFORMANCE ARCHITECTS

Cyber Attack Defender Partners

ForeScout · intel Security · NetApp · riverbed · RSA · vmware · Vormetric Data Security

THE IMPORTANCE OF INTEGRATING YOUR CYBER SOLUTIONS

Cybersecurity professionals are being challenged like never before. They are operating in a rapidly evolving cyber landscape, which requires them to think about new ways to protect, defend and mitigate the impacts of an attack. By taking a new approach to cybersecurity, your agency can build on your existing security infrastructure and tools to implement cost-effective security against today's dynamic threats.

"One cyber challenge is information overload. There is so much information coming in from different alerts, externally from their customers, from security information services about their tools and their environments, it's just an avalanche of information and difficult to navigate," said Jean-Paul Bergeaux, chief technology officer at SwishData Corporation.

Bergeaux is alluding to the challenge of tool sprawl with cyber solutions. Often, government agencies already have many cyber tools deployed, but the solutions have overlapping functions and are not integrated in a way to maximize cyber defense.

That's the problem that SwishData is helping to solve. As a government focused systems integration and data engineering company, SwishData is helping agencies to consolidate and integrate their cyber technologies, eliminate tool sprawl and enable centralized security management across the enterprise. This helps lower the total costs, both operational (OPEX) and capital (CAPEX), of cyber solutions, and allows agencies to develop a more robust cyber defense. Since agencies are able to lower their costs, they can invest in advance cyber solutions like behavioral analytics and anomaly detection.

To start consolidating solutions, organizations must focus on facilitating proper communications between stakeholders. "Often the hardest thing for a lot of agencies to do is to get the right people in the room. This includes employees who are not just cyber security experts, but also project managers and data owners. By bringing everyone to the table an organization can have a cybersecurity summit inside the organization. This will help identify priorities of what needs to be secured and how," said Bergeaux. This is an imperative step for organizations to take and can help them identify the right kinds of solutions to be deployed.

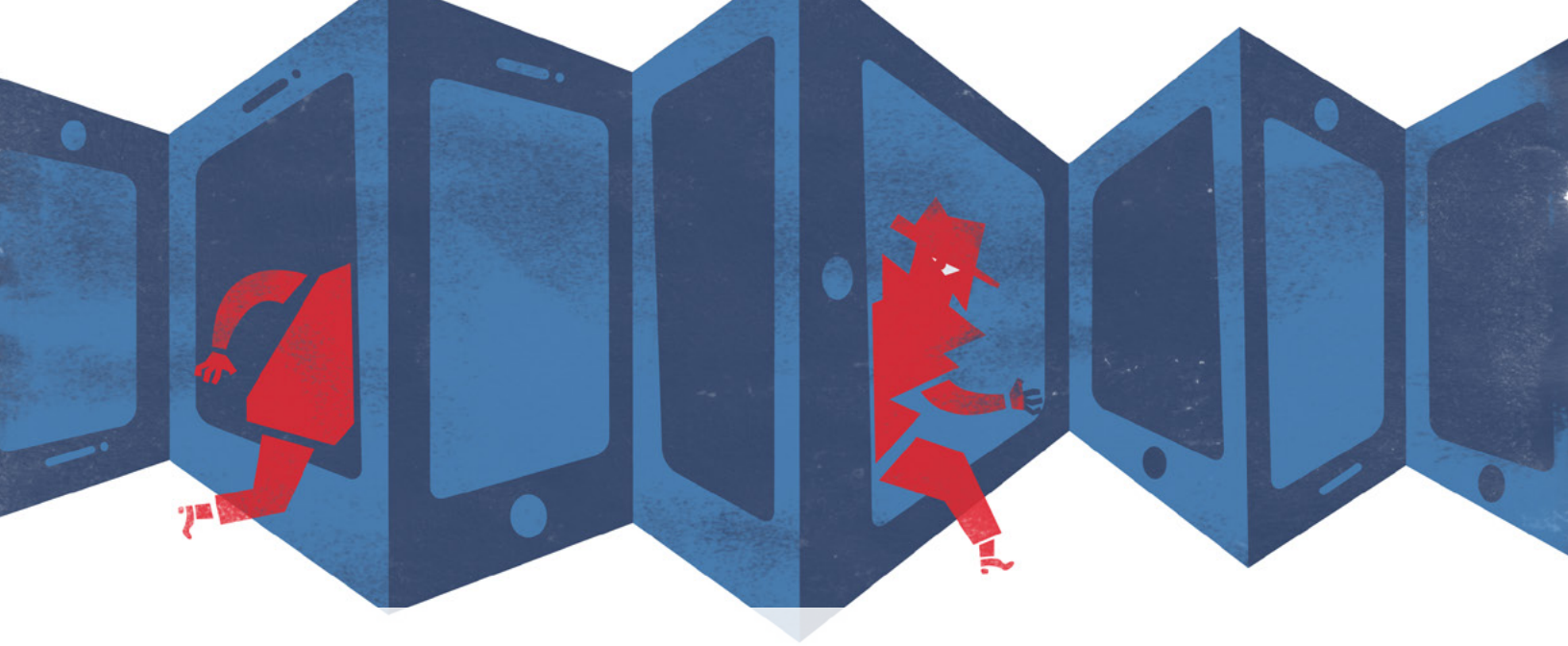
SwishData provides four basic steps to help organizations streamline cyber solutions.

1. Decide Goals: Agencies should determine and prioritize what needs to be protected, and how.
2. Evaluate Environment: Before tools can be selected, agencies must know the products and assess current capabilities. This will help identify untapped features and understand what cumbersome solutions can be replaced.
3. Establish Strategy: It is essential that your agency is able to prioritize investments based on their cost-effectiveness to meet mission requirements and security goals.
4. Achieve Goals: Consolidating cyber solutions will help achieve your goals, and will provide better situational awareness.

As cyber tools become integrated, organizations will then be able to access and share data across tools such as firewalls, IPS, network access controllers, which can be used to improve situational awareness. With this kind of data available, organizations can work towards building a dashboard. With the goal of continuous monitoring, agencies will be able to link all their solutions together and gain a holistic view of the health of an agencies cyber defense. SwishData has made great strides in being a value added re-seller for the cyber market. Their intent is to be a true solutions provider. "There are actually a lot of companies that bring total solutions such as Virtual Desktop Infrastructure (VDI), FDDCI, disaster recovery and backup, and they bring all that together to bring solutions from A to Z, but on the cyber side there aren't really a whole lot of companies that can do that, and that is a huge gap where we have focused," said Bergeaux.

Ultimately, the goal of SwishData is to help find ways to cut the CAPEX and OPEX costs. "We help agencies find ways to improve while you save money, which opens up more funds to further secure your environment. It's about a long view rather than a short view," said Bergeaux. He believes that having a long view is imperative for an agency. "Cyber teams have been underfunded and under the gun, just trying to survive responding to crisis's until recent events allowed them to get enough visibility for more reasonable funding." By creating a multi-year plan, organizations can see the financial impact over the next twelve to eighteen months, and can focus on integrating automation tools, helping to cut costs.

In today's world, it is crucial for organizations to protect their data and information networks. Learning the right way to automate and integrate systems is imperative to the realization of this goal. Although there will be challenges to automating cybersecurity initiatives, it is an essential part of improve an agencies overall security, and keeping information secure.



QUESTION #10: WHAT DO I NEED TO KNOW ABOUT CYBERSECURITY & THE INTERNET OF THINGS?

The Internet of Things (IoT), according to a recent Pew Research Center report, is defined as "a catchall phrase for the array of devices, appliances, vehicles, wearable material and sensor-laden parts of the environment that connect to the Internet and to one another and feed data back and forth automatically." Sounds pretty cool, right? It is — except more connected devices mean more opportunities for hackers and cyberattacks.

Internet-connected devices are expected to number 200 billion by 2020, according to research firm IDC Corp. At that rate, these automated machine-to-machine transactions will outnumber human-to-computer transactions.

As state, local and federal governments make more forays into testing IoT technologies, they'll have to deal with and prepare for the increased cyberattack opportunities, too.

The connected world that IoT brings is bound to improve our lives and create services once believed to be science fiction. But as the scope continues to be realized, many wonder: Is government ready? And more importantly, is government's security ready?

"We are seeing an intersection of different industries with the Internet of Things," said Daniel Castro, senior analyst at the Information Technology and Innovation Foundation, a nonpartisan think tank that promotes public policies to advance technological innovation, in an interview with GovLoop. Many of the industries that are converging have typically not worked together in the regulatory process, Castro said, which makes security alignment even more difficult. Ultimately, though, agencies will be forced to collaborate, which could lead to numerous challenges in creating the necessary regulations, defining the necessary data standards and protecting customer privacy, all of which are imperative to drive innovation with IoT.

"If we thought that doing cybersecurity in a world of wired desktops was hard, now we're going to do it in a world where your coffeemaker, your car and your refrigerator are also a threat vector," said Michael Daniel, a White House cybersecurity adviser, at the 2014 Cybersecurity Innovation Forum. "That makes the problem just that much more difficult."

And the government is already behind the curve. Agencies are also not yet prioritizing IoT as a cybersecurity issue, according to a recent report from the Government Business Council. Less than half of federal executives say their agencies are adapting their cybersecurity strategies to include IoT, and one-quarter say it is a priority.

If and when your agency starts designing products or programs using IoT, the foremost thing they must do is bake in security, said David Jacobs, consumer protection counsel at the Electronic Privacy Information Center, at a recent Federal Trade Commission event.

"What I'm finding is that generally there are two camps," Jacobs said. "That is, there are things that are designed by people who are aware of the kinds of flaws you would find on the Internet, in which case they have a robust design and they address most of the issues and they are quite forward-thinking in terms of what issues you are likely to encounter that haven't cropped up yet. And then there are companies that haven't got the experience, that are coming perhaps from a different industry — maybe, for example, a medical device manufacturer, where they are aware of the issues that you would encounter in the medical device, but are not aware of the issues that they will encounter as an Internet thing. And as a result, they miss a lot of the issues."

Think of this as an opportunity for government to lead. "We can shape, inform, and push that debate, with a fervent commitment to the public good," wrote Abhi Nemani, GovDelivery's civic innovator, in our GovLoop Internet of Things Guide. "Once we accept that the IoT is an inevitability — that consumer service providers will start to instrument the physical world with sensors — there is a compelling advantage to government charting this course along with them. Those institutions — private ones — don't have robust public feedback mechanisms, and are not beholden to the popular will. Our governments are. When they push ahead into this new technological territory, it gives us all a chance to deliberate together around how are rights should be respected and regulated; a precedent hopefully for private sector actors."

QUESTION #11: WHAT'S CRITICAL INFRASTRUCTURE? WHY IS IT AT RISK?

Cybersecurity includes so much more than just credit cards, Social Security numbers and e-mail accounts. Every day cyber defense protects:

1. Broadband networks.
2. Information networks that power business, hospitals and schools.
3. Power grids.
4. Classified government intelligence.

These resources generally fall into the category of critical infrastructure. The National Institute of Standards and Technology describes critical infrastructure as:

> *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.*

Critical infrastructure is the backbone of our nation's economy, security and health. It's used to power our homes, sanitize the water we drink and run the communication systems we rely on to stay in touch with friends and family.

QUESTION #12: WHAT DO I NEED TO KNOW ABOUT THE CONTINUOUS DIAGNOSTICS & MITIGATION PROGRAM?

DHS' Continuous Diagnostics and Mitigation (CDM) program enables government entities to decrease known cyber risks and flaws by expanding their continuous diagnostic capabilities. CDM is poised to make a tremendous impact on government, changing the way agencies combat cyber threats. We encourage you to look at GovLoop's recent report, The Continuous Diagnostic and Mitigation Field Guide, which provides an in-depth summary on the CDM program. But for now, here is some key information on the program:

- DHS has taken on responsibility for CDM, which will enable government agencies to gain increased visibility of their networks. Through CDM, agencies will install sensors to search for known cyber flaws. The results are placed into a local dashboard to create customized reports. Systems are scanned within 72 hours.
- CDM strategically sources tools and Continuous-Monitoring–as-a-Service solutions for civilian agencies.
- The program will lead to improved visibility of network vulnerabilities, risks and flaws, at near-network speed.
- CDM supports efforts to provide adequate, risk-based and cost-effective security solutions.
- Through improved awareness of cyber risks and vulnerabilities, agencies can tackle their hardest challenges first using CDM.

If you're looking for more in-depth resources, be sure to read the GovLoop report.

Information is the key to protecting information. That's why our security solutions are backed by world-class intelligence to help you identify threats in real time and keep your information safe. Learn more at symantec.com/security-intelligence

When you can do it safely, you can do it all.

#GoKnow

Go ahead, you've got Symantec™

Copyright © 2014 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries.

NEW THREATS MEANS NEW SOLUTIONS

Whether it's the ability to pay parking tickets, speeding tickets, file permits, apply or disburse benefits, the internet has transformed the way government delivers services. Although these changes provide much needed relief to citizens, there is also a dark side to digital solutions: the risk of cybersecurity has increased. The digital economy has brought many benefits to citizens, but it also requires government to be more proactive than ever to combat threats.

"We see the threat landscape changing so quickly that it is changing the way we are reacting, and that is actually shaping the landscape of government," said Jen Nowell, Senior Director, Strategic Programs, Symantec Public Sector, in an interview with GovLoop. "One driver is trying to provide many more services to the citizen online. And when doing that, we must be making sure we are focused on identify theft and other security-related issues, as they are now shaping government."

And as government adopts more web services, the way the public sector approaches cybersecurity requirements must evolve. Agencies must take a new approach and think about the variety of ways people access information. That often means they must go beyond checking off boxes for compliance.

"The way things used to be, officials took a checklist approach to security. They would ask, what is the bare minimum I can do to show that I am compliant with government security standards? That's now morphing to something more than just check the box to let's make sure a control is in place, and that it's improving my security posture," said Ken Durbin, Continuous Monitoring and Cybersecurity Practice Manager, Symantec Public Sector.

With programs like Continuous Diagnostic Management (CDM), agencies now use stronger frameworks and controls to protect information and move past the checklist approach. If a breach were to occur, there is much more liability as OMB and related agencies are providing organizations ways to execute cyber initiatives.

The evolution of cyber strategies is important to consider, but as both Nowell and Durbin noted, security does not mean simply deploying a new IT solution.

"We are always talking to our customers trying to find out what their needs are, but it really doesn't end there. They may buy our products, but if they do not deploy them correctly or they are not turning on all the features that are available to them, are they really getting the true protection of the product? I think staying engaged with our customers post sale making sure they are using the products correctly goes a long way in making sure they are improving their security," said Durbin.

Having specific touch points with clients is essential for Symantec, and as their cyber solutions mature, client needs often change.

"Organizations' challenges are always changing, because what the latest vulnerability or threat is right now is always changing. It's different for different customers, and as customers mature in their security program, then they start to experience different things, different threats," said Nowell.

Yet one of the common challenges continues to be network awareness. "The common denominator is that people don't always know what they have. So what I hear most from people is, 'If I could just understand where my network begins and ends, I could then really be able to secure it and lock it down,'" said Nowell.

Durbin added some additional commentary on the challenge of network awareness. "When talking to CIOs and CISOs it is quite surprising when they freely admit they may not have an accurate view of what is deployed on their network, both hardware and software. When you dig a little deeper and ask why, it comes down to priorities, money and the labor force to get it done."

But even when agencies have deployed tools to gain improved network awareness, they are still challenged. "An interesting twist on the problem of network visibility is highlighted by a conversation we had with one agency. They said, 'Look, I got four different tools telling me what's out on my network and they all disagree. I need someone that can help me take those different inventory reports and tell me what I actually have.' So sometimes the issue could be a problem of having too many tools letting you know what is going on," said Durbin.

Having the proper IT solutions and network insights is imperative to securing your agency as well as protecting against emerging threats. By taking some small steps to understand who is on your network, and what IT tools you need to stay secure, your agency can improve its overall security posture, and protect our critical information.

NEXT STEPS: YOUR CYBERSECURITY MUST-READS

There's a lot of great information about cyber on the web. Below, we've pulled together a list of your "must-reads" to be informed. This list also includes sources we used for this report. Use it as a starting point to deepen your knowledge on cybersecurity issues.

- NIST's Cyber-Physical Systems:
  http://www.nist.gov/cps/
- GovLoop's Preparing Yourself for a Connected Government
- FTC workshop: Internet of Things — Privacy and Security in a Connected World:
  http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world
- Comprehensive National Cybersecurity Initiative
  http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf
- The Justice Department's Computer Crime Legal Resources
  http://www.justice.gov/criminal/cybercrime/cclaws.html
- Recommendations of the House Republican Cybersecurity Task Force
  http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf
- The Environmental Protection Agency's Responses to Executive Order 13636
  http://water.epa.gov/infrastructure/watersecurity/upload/EO_13696_10-b-_EPA_response.pdf
- The Health and Human Services Department's Response to Executive Order 13636
  http://www.phe.gov/Preparedness/planning/cip/Pages/eo13636.aspx
- Glossary of Key Information Security Terms
  http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
- "Who Should Lead U.S. Cybersecurity Efforts?" by Kevin Newmeyer
  http://cco.dodlive.mil/files/2014/02/prism115-126_newmeyer.pdf
- Cybersecurity, The White House
  http://www.whitehouse.gov/issues/foreign-policy/cybersecurity
- "Cybersecurity is a Severe and Growing Challenge for Government Contractors," by Eli Sugarman
  http://www.forbes.com/sites/elisugarman/2014/08/26/cybersecurity-is-a-severe-and-growing-challenge-for-government-contractors/
- "The Importance of Cybersecurity to the Legal Profession and Outsourcing as a Best Practice — Part One," by Ralph Losey
  http://e-discoveryteam.com/2014/05/11/the-importance-of-cybersecurity-to-the-legal-profession-and-outsourcing-as-a-best-practice-part-one/
- "Risk Mitigation Strategies: Lessons Learned from Actual Insider Attacks," by Dawn Capelli and Andrew Moore, Software Engineering Institute, Carnegie Mellon University
  http://resources.sei.cmu.edu/asset_files/Presentation/2008_017_001_52131.pdf
- Combating the Insider Threat at the FBI: Real World Lessons Learned
  https://media.blackhat.com/us-13/US-13-Reidy-Combating-the-Insider-Threat-At-The-FBI-Slides.pdf
- Be Sure to Look Around the Office When Searching for Gaps in Your Data Security, Robert Siciliano.
  http://www.entrepreneur.com/article/236162
- Cyber Security Planning Guide, Federal Communications Commission
  http://transition.fcc.gov/cyber/cyberplanner.pdf
- The 11 most common computer security threats…And what you can do to protect yourself from them, Norton Symantec.
  http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx
- Prepare for the Attack of the Data-Sucking Cyber Zombies, Andrew Van Noy
  http://www.entrepreneur.com/article/237142
- How to Respond to Cyber Attacks on Your Business, Gene Quinn
  http://www.ipwatchdog.com/2014/01/27/how-to-respond-to-cyber-attacks-on-your-business/id=47603/

ABOUT GOVLOOP

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

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

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

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

www.govloop.com
Twitter: @GovLoop

ACKNOWLEDGMENTS

Authors: Catherine Andrews, director of content, Pat Fiorenza, senior research analyst. Matt Garlipp, research fellow, Hannah Moss, research analyst, Corinne Stubbs, brand ambassador.

Designers: Jeff Ribeira, senior interactive designer, GovLoop, Tommy Bowen, junior designer, GovLoop, and Jake Brennan, design fellow, Govloop.

Editor: Catherine Andrews, director of content, GovLoop

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