How to Play Your Role in Cybersecurity

govloop

Table of Contents

Worksheets

Executive Summary

The 2018 "Enhancing the Resilience of the Internet and Communications Ecosystem" report to the president clearly states:

> "To enhance the resilience of the Internet and communications ecosystem against distributed threats, all stakeholders must recognize and be prepared to execute their roles and responsibilities."

Cybersecurity is not a strategy to be executed in the back offices of agency IT departments. While technology and security professionals continue to play a leading role in securing government information, cybersecurity depends on every agency employee today. The escalation of cyberattacks, both in volume and sophistication, makes it imperative that every public servant has an eye on security.

Frontline employees must secure their devices, follow cyber hygiene protocols and help identify potential insider threats in real time. Procurement professionals must ensure that everyone has the right technology and that it's easy to secure from the time of deployment. Agency leaders must create and enforce robust cyber policies that tackle threats holistically, coordinating across technological, organizational and cultural aspects.

And that's just the beginning. Every person in a government organization has a part to play in the cybersecurity mission.

This playbook explores six tactics to create an agencywide culture of cybersecurity, including:

1. Assessing organizational security.
2. Outlining the basic security expectations of your agency
3. Creating a culture of transparent cybersecurity
4. Choosing the best technologies to empower secure use
5. Ingraining security into daily operations and processes
6. Tracking performance and engagement for long-term cyber success

This guide also includes best practices from government experts at the state and federal levels to help spread cybersecurity beyond the walls of IT. It also outlines the tools and teams you'll want to assemble for each step of your cybersecurity journey, and provides worksheets to get started.

Cybersecurity is now part of everyone's job description. This playbook will help your agency enable every employee — from frontline staff to the top administrator — to safeguard government.

Our Government Experts

Neil Carmichael
Director of the Insider Threat Program
Office of the Chief Operating Officer
National Archives and Records Administration

Joseph Kirschbaum
Director
Defense Capabilities and Management
U.S. Government Accountability Office

Chris Hill
Acting Chief Information Security Officer
Department of Innovation and Technology
State of Illinois

Todd Nacapuy
Chief Innovation Officer
State of Hawaii

Debbi Blyth
Chief Information Security Officer
State of Colorado

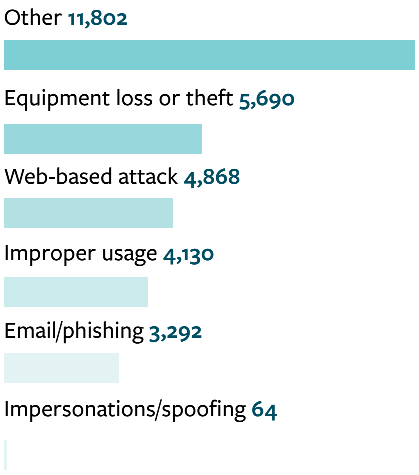
The State of Cyber

● State & Local

● Federal

Risks & Attacks

● FY 2016 Agency-reported incidents by attack vector



Other 11,802

Equipment loss or theft 5,690

Web-based attack 4,868

Improper usage 4,130

Email/phishing 3,292

Impersonations/spoofing 64

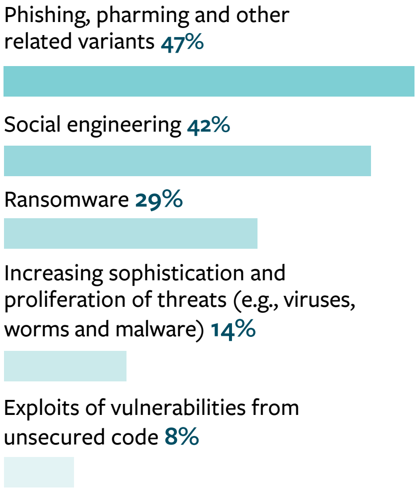
● 56%

Decrease in reported security incidents in 2016

● 30,899

Cyber incidents that led to the compromise of information or system functionality in 2016

● Prevalence of cyberthreats across state governments



Phishing, pharming and other related variants 47%

Social engineering 42%

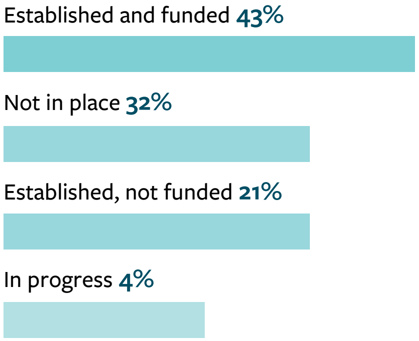
Ransomware 29%

Increasing sophistication and proliferation of threats (e.g., viruses, worms and malware) 14%

Exploits of vulnerabilities from unsecured code 8%

Strategies & Spending

● Cybersecurity incident/data breach reporting and handling



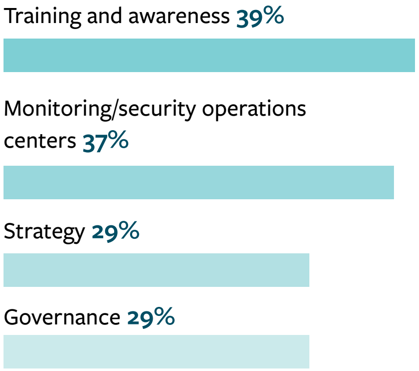
Established and funded 43%

Not in place 32%

Established, not funded 21%

In progress 4%

● Top cybersecurity initiatives for 2016



Training and awareness 39%

Monitoring/security operations centers 37%

Strategy 29%

Governance 29%

● 7,500

Cybersecurity and IT employees hired by agencies in 2016 versus 5,100 in 2015

● 100%

CFO Act agencies implemented policy to ensure that all employees with access to information receive privacy training

● 90%

Non-CFO Act agencies implemented policy to ensure that all employees with access to information receive privacy training

● $19 billion

Allocated for cybersecurity in the 2017 budget

● 70%

Federal agencies that have employed strong anti- phishing and malware capabilities to help safeguard their networks from malicious activity

● 62%

State government respondents who said a lack of skilled personnel is a "major challenge"

● 81%

Government users now using multi-factor Personal Identity Verification cards to access federal networks

Play 1: Assess Your Organization

The Play

Especially if a pressing deadline is approaching or a breach has recently occurred, it can be tempting to immediately deploy new cybersecurity tools and tactics to safeguard your agency. But no matter what scenario has caused agency leaders to rethink cybersecurity, it's critical to take the time and effort to assess the current risk of personnel, systems, processes and information.

This first play is important for multiple reasons. First, government is short on both IT budget and trained security staff. That means agencies can't afford to apply costly blanket solutions across the organization if there isn't a true need. By identifying where risk is higher, leaders can prioritize resource allocation, securing the most vulnerable areas first without overstretching the budget and staff.

Second, a risk assessment is necessary to provide a baseline of performance. As future security investments are made, cyber personnel need to know what's working and what's missing the mark. They can do that only if they have a gauge of past performance by which to compare security.

For these two reasons, many regulations such as the Federal Information Security Management Act (FISMA) and federal cross-agency priority (CAP) goals require agencies to perform and report on routine cybersecurity assessments.

How to Do It

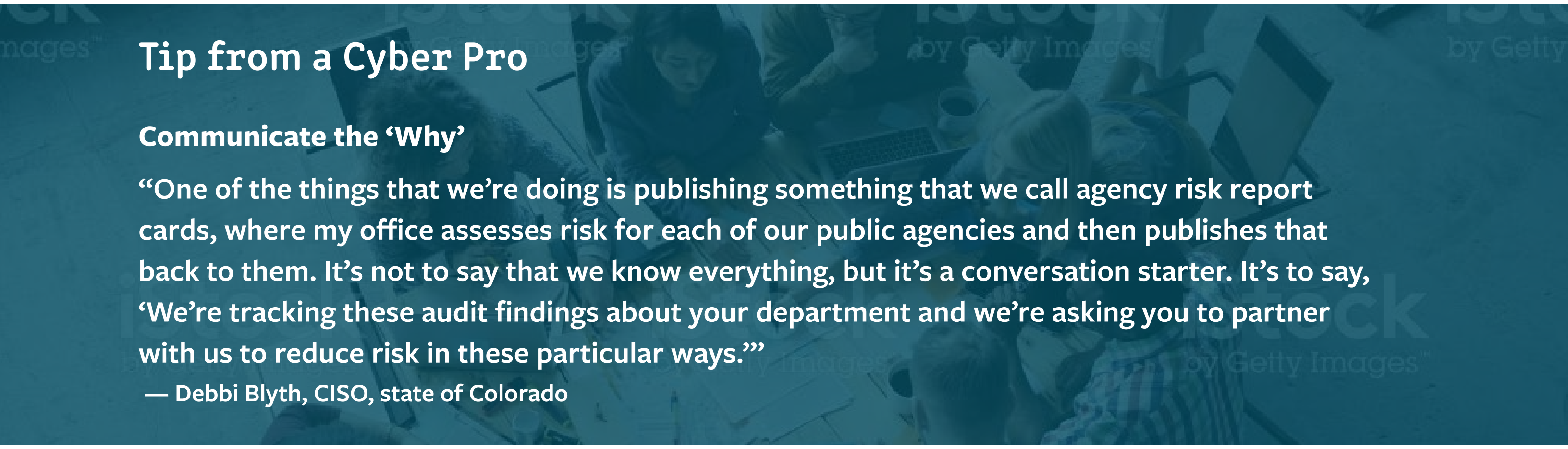
To achieve the objectives in this play, you'll want to choose an assessment model — that is, the standards by which you will judge risk — and recruit personnel to help you execute that evaluation.

Luckily, you don't have to start from scratch. Because cybersecurity is so critical to government operations, many frameworks are already designed to guide agency leaders in assessing risk.

For instance, when the Government Accountability Office's Defense Capabilities and Management division started looking at defense insider threat programs, Director Joseph Kirschbaum said they used the National Insider Threats Taskforce minimum standards as a baseline to gauge efficacy. The Risk Management Framework for DoD Information Technology also provides baselines for defense agencies to consider non-insider security risks.

For civilian agencies, the National Institute of Standards and Technology (NIST) routinely updates its Cybersecurity Framework, which offers guidance on identifying and mitigating risk at all types of organizations, including private-sector and non-federal agencies.

Once leaders decide on a framework, they must communicate the assessment — both its tactics and its value to the organization — to personnel at all levels. This communication not only drives awareness regarding cybersecurity, it also serves as the first step toward recruiting those employees to help with future cyber tactics.



Tip from a Cyber Pro

Communicate the 'Why'

"One of the things that we're doing is publishing something that we call agency risk report cards, where my office assesses risk for each of our public agencies and then publishes that back to them. It's not to say that we know everything, but it's a conversation starter. It's to say, 'We're tracking these audit findings about your department and we're asking you to partner with us to reduce risk in these particular ways.'"

— Debbi Blyth, CISO, state of Colorado

The Team

Program Managers
Provide relevant information to security personnel and communicate rationale for security assessment to non-IT staff

Non-IT Senior Leaders
Highlight that cybersecurity isn't just an IT issue, and help recruit non-IT staff to the cyber mission

Information Security Officer
Deploys and coordinates the risk assessment, ensuring that all relevant information is consolidated in a single office for holistic analysis

The Tools

Networking
Connects systems to one another and to a central database, usually via software-defined networking, for analysts to collect information regarding their functions and security

Data Analytics Platform
Collects information from across agency systems and compiles it in a single location for analysis of security events and connections

Talking Points

This is important because...

"we don't know what our risks and vulnerabilities currently are, or how to better secure our systems. We have to know where we are before we can move forward."

After investing in this tactic, our agency can expect...

"to create a more efficient and cost-effective cybersecurity strategy that prioritizes the greatest areas of vulnerability, rather than applying blanket tactics across the organization."

Play 2: Outline the Basics

The Play

As you complete your assessment, it should become clear where your agency is excelling and where more work needs to be done. With that understanding, it's time to put pen to paper. Outline what the security posture of your agency will be and how it will be achieved.

The basics of your security policy will answer these questions: What risk is acceptable for which systems and information? What must employees do to maintain or decrease that level of cyber risk? How should tools and technologies be used to safeguard information?

Some of the items that will comprise your security policy and best practices, like applying firewalls and patches to relevant systems, will fall to IT personnel. Other practices, such as network traffic monitoring, can be automated to decrease staff burden while increasing security.

However, many other items, such as routinely changing strong passwords or shutting down desktops before leaving the workplace, will become the responsibility of all employees. Clearly outline cyber hygiene best practices and expectations for all personnel, making it clear how to achieve them and where to get more information.

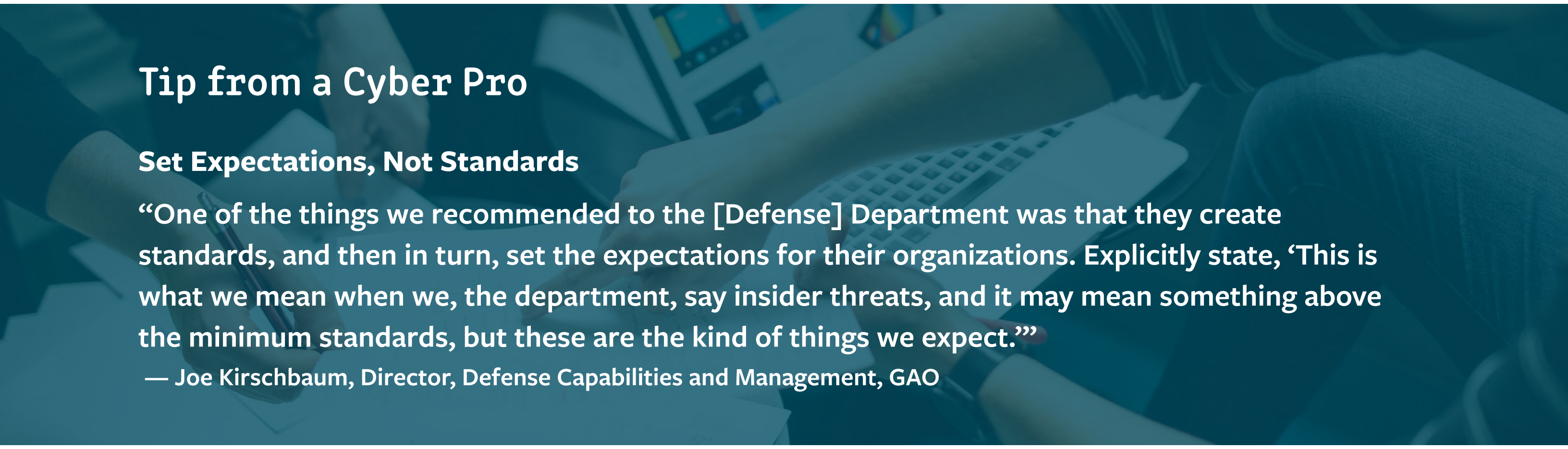
How to Do It

The most important part of this play is communication. First, ensure that your messaging on expectations doesn't just come from the IT or cybersecurity office. For non-IT staff to buy into cybersecurity goals, they should hear directly from their own supervisors and department leaders how those goals affect their missions and business objectives.

Where possible, standardize the alignment of those goals. Illinois Acting CISO Chris Hill said it's been critical to the state's cybersecurity success that non-security leaders recognize the need to integrate security into plans. In fact, cybersecurity has been wrapped into Smarter Illinois, an initiative to digitally transform state technologies and services.

Additionally, make sure communication of expectations is not a one-time event. Routinely emphasize the importance of cybersecurity across mission functions, and how non-IT personnel can achieve it. This often involves training. Colorado CISO Blyth, for example, said her agency hosts quarterly cybersecurity training to keep cybersecurity top of mind for employees and to enhance their ability to safeguard systems. Courses are tailored to the access privileges and roles of individual employees.

Finally, consider passive ways to keep employees thinking about cybersecurity. The District of Columbia's government recently created a series of posters that hang in city buildings to remind personnel of cyber risks and strategies. But even without a design team, you can create a simple cyber hygiene checklist that can remind employees of best practices each day. (See worksheet, Page 23).



Tip from a Cyber Pro

Set Expectations, Not Standards

"One of the things we recommended to the [Defense] Department was that they create standards, and then in turn, set the expectations for their organizations. Explicitly state, 'This is what we mean when we, the department, say insider threats, and it may mean something above the minimum standards, but these are the kind of things we expect.'"

— Joe Kirschbaum, Director, Defense Capabilities and Management, GAO

The Team

CIO

Sets baseline cybersecurity expectations, plus procedural and access management guidelines, for the entire agency

Human Resources

Ensure personnel are introduced to security during onboarding and routinely educated on cybersecurity policies throughout their tenure

Communications

Translates agency expectations and standards to non-IT personnel and external stakeholders

The Tools

Employee Intranet

Provides a central repository where employees can access cybersecurity guidance, requirements and other information as they need it

Learning Management System

Collects information from across agency systems and compiles it in a single location for analysis of security events and connections

Communications Platform

Provides integrated communications mediums, including but not limited to email, to relay messaging organizationwide in accessible formats

Talking Points

This is important because…

“we need everyone to be on the same page about what cybersecurity means for our organization and how they can get involved in achieving that goal.”

After investing in this tactic, our agency can expect…

“more employees to understand the role they play in cybersecurity, as well as what acceptable, secure behavior looks like.”

HOW CAN YOUR AGENCY INCREASE SECURITY WITHOUT ADDING COMPLEXITY?

FEDERAL AGENCY NETWORKS SUPPORT missions worldwide—from the desktop to the field, and cyber security must be a top priority. Running legacy security systems increases complexity, resource needs, and risk.

Fortinet Federal is the only company with integrated security solutions for networks, endpoints, applications, and clouds designed to work together as a collaborative fabric. Simplified management and fast, automated response save time and deliver better threat protection.

Learn how your agency can get better protection with an adaptive and intelligent security fabric for seamless, end-to-end protection that meets the evolving demands of the mobile Federal workforce.

FORTINET®

FORTINET SECURITY FABRIC
Network, Endpoint, Application
and Access Security

www.FortinetFederal.com

Partnering for Security in the Cloud

An interview with Felipe Fernandez, Director of Systems Engineering at Fortinet Federal

For many agencies, cloud computing is a vital component of their IT strategy because it provides the flexibility and scalability government needs to meet modern technology demands. But while there are significant benefits of the cloud, agencies must be careful not to sacrifice security during cloud migration.

To learn how organizations leverage the flexibility of cloud without decreasing their security posture, GovLoop sat down with Felipe Fernandez, Director of Systems Engineering at Fortinet Federal. Fortinet Federal provides solutions and services to help agencies build robust cybersecurity.

"The one thing agencies need to realize is that the cloud, in terms of how it's architected, is very different from their legacy networks," Fernandez said. "They have to educate themselves and adapt to the new architecture on which their applications will be deployed and defended."

He explained that operating in the cloud inherently means working with an abstracted layer of equipment and understanding that applications are running on potentially shared hardware resources. Additionally, depending on the cloud configuration and licensing agreement, agency users may have more or less control over how shared resources and data are accessed.

Those unique aspects of cloud must be considered as agencies update their cybersecurity approaches, processes and tools. For instance, service contracts must be created to strictly outline ownership of data and systems, both during migration and at system end-of-life. Additionally, cloud providers must be scrutinized to ensure they consistently maintain resilient technologies that safeguard every component of the cloud.

Finally, IT teams within agencies have to ensure that systems connected to or relying on the cloud are orchestrated to endure breaches or failures. For instance, if a cloud service is hit by a severe denial of service (DoS) attack, administrators should be able to quickly redeploy affected applications in another environment to maintain both performance and security.

Often, it will take multiple solutions provided by different vendors to create holistic cybersecurity during cloud migration and maintenance. To navigate those disparate technologies and processes, Fernandez recommended seeking help.

"There are two factors to weigh equally in your strategy. The first is having a trusted, experienced migration partner that has achieved a certified status with a cloud provider," he said. Migration partners take the burden off of agency IT staff by coordinating and integrating all necessary technologies to ensure cybersecurity is upheld during a cloud migration. Rather than working with multiple vendors to procure separate solutions, agencies can work with this single partner to form a holistic approach to security.

Moreover, migration partners who have certified status with individual cloud providers are in a better position to determine which solutions will best support unique environments. For instance, Fortinet Federal has experience working with Microsoft's Azure for Government, Amazon Web Services, as well as other common government cloud services.

"Then, it's important to use available government checklists and mandates as factors to calculate whether or not you've securely deployed your applications in the cloud," Fernandez continued.

As more agencies embrace cloud, the federal government has created a number of security aids, as well as standards and regulations, to safeguard those transitions. This both helps and complicates many cloud journeys. On a positive note, when agencies meet these standards, they can rest assured that their cloud environments are secure. Regulations like FedRAMP clearly outline what security in the cloud should look like.

However, it can be cumbersome for agencies to navigate the ever-growing and changing list of regulations. Again, a trusted migration partner can be helpful here. Because they have experience with government compliance standards, partners like Fortinet Federal can efficiently identify certified solutions that will meet an organization's regulatory needs.

Finally, Fernandez pointed out that by enlisting a third-party migration partner, agencies can actually decrease their overall costs. Agencies will have to dedicate fewer IT staff and labor hours to cloud migrations or management, and they don't have to worry about unexpected failures that would take additional resources down the road. At the same time, these partners can leverage their long-standing relationships with cybersecurity and cloud vendors to ensure the appropriate solutions are acquired at the lowest price point.

Migration partners not only help agencies leverage the cloud; they also ensure they get the most out of their investment. "Our top priority at Fortinet Federal is ensuring that cloud migrations aren't causing a lack of performance or a degradation of security," Fernandez concluded. For government to move forward with cloud, cybersecurity must remain a top priority, and that can only be achieved through effective partnerships with trusted providers.

Play 3: Create a Culture of Transparency

The Play

Related to the need to clearly outline expectations is the imperative to transparently organize and execute your cybersecurity strategy. In interviews with multiple government leaders, they said the most common roadblock to ingraining security across an organization was lack of employee buy-in due to misconceptions about how to achieve cybersecurity.

"When we talk about monitoring, the first thing that comes into play is politics, because people are under the impression that Big Brother is watching over them," said Illinois CISO Chris Hill. "That's not the message we're wanting to sell. We need them to know that we're actually trying to deliver a service."

Staff members often misunderstand the tactics and intent of monitoring — core components of ongoing cybersecurity. As a result, they may seek ways to circumvent monitoring procedures or opt out of security programs where possible. But if agencies clearly explain why systems are monitored — and what information they're specifically concerned about and how it's collected — employees are more likely to participate.

In addition to encouraging employees, transparent cybersecurity strategies can help them take ownership of cyber strategies. If employees understand what to look for, where to report it and how to decrease risk, they can become valuable partners in the fight for a more secure government.

How to Do It

There is no one-size-fits-all strategy for transparently crafting cybersecurity. Different organizations will have different security needs and staff with different levels of technical know-how. The key is to tailor your messaging to those varying demands.

In Hawaii, State Chief Innovation Officer Todd Nacapuy said government employees are categorized by what type of technology — mainframe, PC, laptop or mobile — was dominantly used when they started working for the state. Any new IT project is communicated in a way that's tailored to that generation, giving them more or less information in technical or laymen's terms, depending on their preference. That means the cybersecurity tactics and considerations associated with any new initiatives are appropriately translated for the audience, ensuring they understand and can deploy their requirements.

In Colorado, Blyth said they train personnel on specific issues that affect their systems. "So, for individuals related to projects asking for changes to firewalls, we train them on changes that we make to firewalls, what it means, what the risk could be, what types of rules apply and what types of information that we're looking for," she said.

Finally, Neil Carmichael, Director of the Insider Threat Program at the National Archives and Records Administration's Office of the Chief Operating Officer, took the direct approach of simply talking with stakeholders. "I met with every executive that would need to provide us information. So, it was our human capital, it was our business support and it was our IT folks. I talked to them about what they could provide us, what that would look like and how the data would be used," Carmichael said.

Tip from a Cyber Pro

Explain Connections

"There are vulnerabilities [such as mobile device access] that don't necessarily manifest themselves as cyber vulnerabilities, per se. But it's nevertheless a security vulnerability for the soldier, sailor, airman or Marine, and that's important for security folks to know about. Getting individual silos to appreciate that and plan for those dependencies is really the key to a cross-disciplinary approach."

— Joe Kirschbaum, Director, Defense Capabilities and Management, GAO

The Team

Program Managers
Form the first line of communication and defense for your frontline employees

Help Desk
Creates a clear contact within your IT shop to field concerns and respond to potential phishing emails or other attacks frontline staff report

Security Officers
Communicate and clarify rules related to cybersecurity

The Tools

Ticketing Systems
Provide a direct route for employees to easily alert IT or cyber staff to potential threats

Plain Language Tools
Help translate complex and technical ideas into relatable messaging for personnel and external stakeholders with any knowledge level

Tip from a Cyber Pro

Be a Resource

"A lot of it is really just being open to communication. It's just a matter of listening to the group — really listening to what they're saying — and then try[ing] to address it to keep that communication and dialogue open."

— Neil Carmichael, Director, Insider Threat Program, NARA

Talking Points

This is important because…

"employees need to understand how they can contribute to effective cybersecurity strategies, rather than just hoping our IT personnel will take care of problems."

After investing in this tactic, our agency can expect…

"employees to be more vigilant and participative when it comes to cybersecurity programs, rather than trying to circumvent security procedures."

Play 4: Choose the Right Technology

The Play

Estimates vary between 24 percent and 60 percent, but there's no doubt that a significant portion of cybersecurity incidents are the result of employee error and technology misuse. That's not because a large portion of public servants want to subvert government. More often, employees simply don't know how to use agency technologies.

Training can help, but it can only go so far. Employees are especially prone to circumvent security protocols for the sake of efficiency if it's complex to securely use technologies, such as needing multiple passwords across devices or to manually encrypt sensitive information.

The goal of this play is to take the burden off employees. Instead, equip them with tools that make it easy for them to securely complete their daily tasks.

What does the right technology look like? First, it should have security built into its architecture, rather than added on after procurement. That eliminates integration concerns and makes it easier for cyber professionals to maintain system security.

Second, employee-facing technology should be usable by any user, regardless of their technical expertise. As NIST describes, a usable technology "needs to make it easy for the user to do the right thing, hard to do the wrong thing, and easy to recover when the wrong things happen anyway."

How to Do It

A portion of this play relies on your acquisitions team. Ensure that every procurement — including those that don't have an obvious connection to sensitive information gathering or critical systems — is examined for cybersecurity risks, and for safeguard and security measures to prevent against future risks.

But when it comes to ensuring that new technologies are accessible to novice users, the responsibility lies with a host of people, including acquisitions, security and IT professionals, and software designers. Even program managers can participate in this play by calling out difficult-to-use technologies and suggesting improvements.

Working in concert, these groups should procure or update technologies that enable secure use. For instance, the state of Colorado has deployed automatic alerts to employee email systems that notify users if they might be sending sensitive to the wrong recipients. Encryption is also automatically applied to sensitive data before it leaves the network.

To determine the usability of your technologies — whether they are acquisitions in consideration or tools already in use — test them with employees. Usability.gov offers a wealth of resources to help government designers, project managers, engineers and content creators make more usable products and services.

The most commonly used usability test, the System Usability Scale (SUS), was created in 1986 and is still used by the government today. Although SUS determines only ease of use without considering security, it can be altered to incorporate cybersecurity factors. (See example on Page 24.)

Tip from a Cyber Pro

Dont Forget People

"We're talking about very technical issues, and very complex topics. But you can never forget or lose sight. This is a human problem; we're dealing with humans, interacting with a piece of equipment. That should be a fundamental framework to keep in mind."

— Joe Kirschbaum, Director, Defense Capabilities and Management, GAO

The Team

User Experience

Determines and upgrades the usability of internal tools and interfaces, in addition to scrutinizing citizen-facing applications and services

Procurement Officers

Standardize acquisition processes, regulations and requirements to ensure that security is built into technologies before deployment

Engineers and Developers

Design or update programs to make them more user-friendly without sacrificing security

The Tools

Automation

Removes the potential for human error in turnkey cybersecurity tasks such as encryption, patching and password updates

Usability Testing Software

Performs analytics on user behaviors to understand how and which actions a website or service's design promotes

Surveys

Can easily and inexpensively help identify employee sentiments regarding current technologies and ease of security

Talking Points

This is important because...

"we can't rely on our non-IT staff to know every security concern associated with our tools and how to correct them. We have to make it easy for them to help us secure our agency."

After investing in this tactic, our agency can expect...

"our employees to be happier with the technologies they use, even as we better secure our infrastructure and systems."

solarwinds
federal

Mount a better defense

with SolarWinds cybersecurity & continuous monitoring solutions

Agencies are under increasing pressure to identify and protect against internal and external cybersecurity threats, as well as detect, respond, and recover from incidents.

SolarWinds® solutions help you improve your agency's Risk Management Framework (RMF), NIST 800-53 controls, FISMA, and DISA STIGS compliance. They also help you implement, assess, and monitor your security controls to better defend against attacks, and continuously monitor your networks, systems, and application for compliance.

Join nearly every civilian agency, DoD branch, and intelligence agency in using SolarWinds' powerful, affordable, and easy-to-use solutions to make government IT more secure:

Log & Event Manager

User Device Tracker

Patch Manager

IP Address Manager

Network Configuration Manager

Secure Managed File Transfer

Click here to learn more about how SolarWinds addresses federal cybersecurity.

IT management & monitoring solutions for government

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

Go to solarwinds.com/federal to download fully-functional free trials
877.946.3751 federalsales@solarwinds.com solarwinds@dlt.com

© 2018 SolarWinds Worldwide, LLC. All rights reserved.

SOLARWINDS FEDERAL DISTRIBUTOR DLT

Moving Beyond Compliance to Ensure Security

An interview with Paul Parker, Chief Technologist – Federal and National Government at SolarWinds, and Don Maclean, Chief Cybersecurity Technologist at DLT Solutions

It's no longer a question of whether agencies are at risk of a cybersecurity attack. Instead, organizations are focusing on managing and countering the inevitable threats facing their systems and data. But how can they prevent attacks when they're not sure how or when they will happen?

Taking a risk management, continuous and holistic approach to cybersecurity is one answer. In a recent interview with Paul Parker, Chief Technologist – Federal and National Government at SolarWinds, and Don Maclean, Chief Cybersecurity Technologist for DLT Solutions, we asked what it took to adopt a risk-management approach to cybersecurity. They encouraged government IT professionals to look beyond regulatory guidance to adopt automated continuous monitoring. Together, DLT and SolarWinds provide the tools to do that.

One obstacle facing many agencies is the confusion between compliance and security. The federal government has created a number of mandates and regulations to guide agencies, including the NIST Risk Management Framework. However, as more regulations are developed, IT professionals are becoming overwhelmed with information.

According to SolarWinds' 2017 Federal Cybersecurity Survey, public servant IT processionals feel the same. Over half of respondents (52 percent) indicated that regulations and mandates posed more of a challenge to managing risk than in the past, and respondents were twice as likely to feel that the Risk Management Framework posed a challenge to managing risk than helping contribute to cybersecurity success.

But more than simply inundating security professionals with information, Maclean and Parker said that these regulations can mislead agencies by conflating compliance with effective risk management. "It's become a big focus on just checking the box," Parker said. "It's not about knowing you are more secure or less secure. It's about meeting the mandates and deadlines."

"The Framework was supposed to be a jumping off point, where agencies could understand what was wrong and begin to fix it. But the processes became so exhaustive that compliance became an end in itself," Maclean added.

Luckily, more government IT professionals are starting to understand the potential disparity between compliance and security. In the same SolarWinds survey, 70 percent of respondents felt that being compliant does not necessarily mean being secure.

Parker and Maclean agreed that agencies must move beyond regulatory standards to invest in automated, continuous monitoring. This is especially critical as agencies encounter more cyberthreats from within their organizations. "Insider threats are always going to be one of the top threats for agencies," Parker said.

More than half of survey respondents (54 percent) said that careless or untrained insiders represent the greatest security threat to their agency, while 29 percent felt that malicious insiders were also a significant threat.

Continuous monitoring can help prevent and detect both intentional and accidental misuses of agency technologies and information. By monitoring technology use, network traffic, and other IT log data, administrators can better understand the baseline operations of their network as well as identify irregular data that might indicate a threat.

At the same time, administrators can more reliably counter risks that are detected, as automated technologies reduce the potential for human error and system misuse. Plus, automation of manual tasks saves IT staff significant time and labor, allowing them to focus on the higher-risk threats against their networks.

However, automated continuous monitoring requires more than simply placing sensors throughout an agency network. It requires a collection of security tools deployed across an organization, working in concert to collect and synthesize a diverse array of data.

"There's a lot of exhaustion around the number of products on the network today," Parker said. "What many agencies are really missing is the most basic network security. That's where SolarWinds can really help. We can bring in easy to use, affordable IT management solutions that help address many of these gaps."

With an integrated and mapped technology suite of network monitoring tools, IT staff can quickly analyze data from across the entire organization and react to insider threats in real time. They can reap the benefits of automated network monitoring, without getting lost in individual product details or worrying that systems connected properly.

That also helps agencies report reliably to regulatory bodies on their progress towards cybersecurity compliance. With a confident, risk-based network security strategy, organizations can move beyond simply checking the box on regulations. They can begin to tackle the real insider threats facing government today.

Play 5: Operationalize Security

The Play

Security is not a one-off event. It must be a component or consideration of every task employees execute, even when that task might seem unrelated to cybersecurity. The tools in Play 4 can certainly help with that by offering security reminders and making it easier to safeguard systems. However, agencies must also take an operational approach to security if it is to be a consistent part of every department's functions.

Operationalizing security requires creating processes to ingrain security in all daily operations, such as procuring new technologies, integrating new systems or even onboarding new employees. Ensure that the processes surrounding each event force personnel to consider the security implications of their actions and report relevant information to IT or security departments.

Additionally, operationalized security involves planning for unexpected events. A major component of cybersecurity is being ready to quickly respond to a technology failure, security incident or breach. Having your personnel equipped with procedures to quickly minimize damage and connect to security teams can ensure security isn't sacrificed in one-off, unexpected events.

How to Do It

Operationalizing security can require strategically updating organizational structures and processes. First, agencies must consider how current structures allow non-IT personnel to impact and interact with other groups. It's imperative that cybersecurity officials be able to quickly and directly enforce standards and educate staff.

This may require moving cybersecurity away from IT. For instance, the National Archives Insider Threats Program Director, Neil Carmichael, reports directly to the agency's COO. He said that setup is particularly beneficial because it shows that cybersecurity is not only an IT problem. It also allows the Insider Threat Program to access data from across the organization.

However, organizational structures don't always have to be overhauled to operationalize security. Granting security personnel more access by standardizing procedures can also achieve better cohesion among disparate departments.

For example, Colorado's Blyth said her department works to standardize procurement events that must get the department's seal of approval before execution. Rather than placing security officers in every department or on every contract, Blyth's office routinely evaluates their request for proposals templates if they realize a relevant event bypassed information security scrutiny. They then update the standard RFP, in addition to related service provider contracts, to include those circumstances, so the next event will automatically go through the office before execution.

Tip from a Cyber Pro

Grant Ownership

"In order to modernize state government, we need to give our people tools to do that. But at the same time, we need to also enable them to change the processes to make the government more effective and efficient."

— Todd Nacapuy, Chief Innovation Officer, state of Hawaii

The Team

COO

Grants authority for IT and security personnel to alter and standardize operations that aren't obvious cybersecurity concerns

Procurement

Ensures security standards are upheld at every stage of technology acquisition and can be easily integrated with other secure tools and processes

Program Manager

Provides insight into on-the-ground, daily processes and identifies areas for security improvement

The Tools

Program Management Software

Allows agency stakeholders to share process information and track operations from a single system, creating better shared understanding

Identity Access Management

Automatically elevates or removes users' access privileges as their roles change, rather than requiring IT personnel to routinely audit credentials

Network Mapping

Enables IT professionals to identify cybersecurity connections and dependencies among technology systems

Talking Points

This is important because...

"security is an organizationwide concern. If we don't include it in our standard operations throughout departments, we're likely to miss a cyber risk that could really impact the agency."

After investing in this tactic, our agency can expect...

"to have more confidence that daily operations aren't creating unknown risks for our agency and that one-off events are being reported to us."

Play 6: Track Performance

The Play

Setting expectations, operationalizing processes and equipping employees with tactics and tools to pursue security are ongoing efforts that require revision as scenarios change, needs fluctuate or — most importantly — it turns out that a tactic simply isn't working.

Ongoing performance tracking is a must for stakeholders, including IT security personnel and agency leaders, to know when cybersecurity strategies need course correction. But it's important to understand that this play isn't just about monitoring security dashboards to see when and how breaches occur.

Remember the basic expectations outlined in Play 1? Those people, process and technology standards should not only set a baseline to start your cyber journey, but also be used to measure cybersecurity understanding and employee behavior in real time. Are policies being effectively implemented? Are non-IT staff understanding and embracing them?

To make sure you're addressing the human element of cybersecurity across your organization, performance tracking is just as much about tracking engagement and adoption as it is about tracking security alerts from IT.

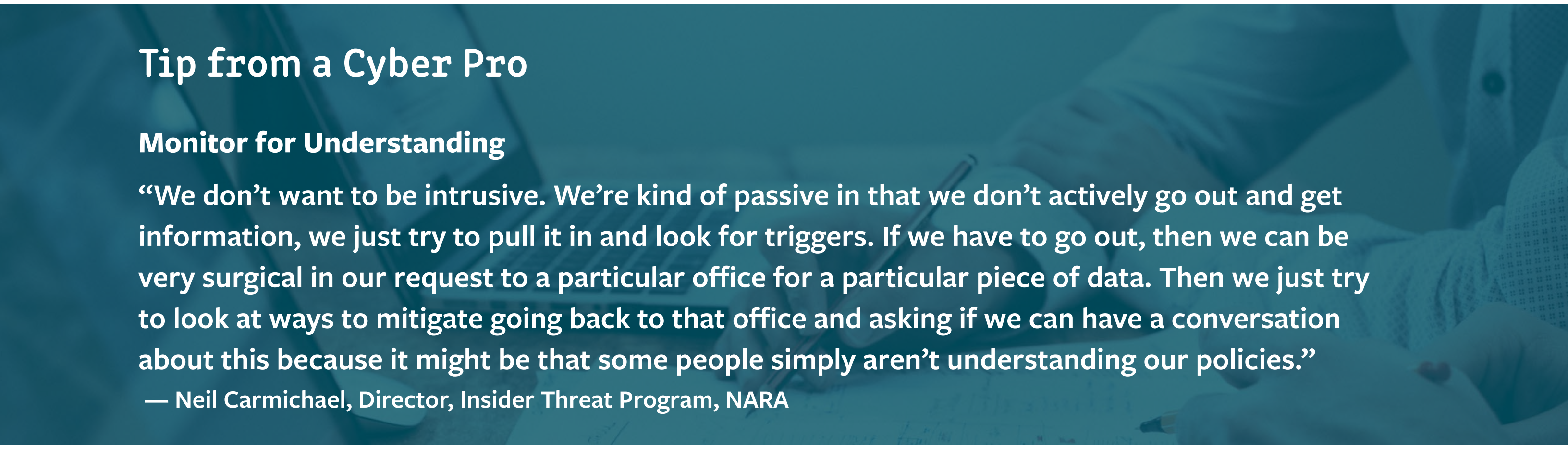
How to Do It

A central component of performance tracking is analyzing the data the personnel and systems of your agency generate to determine where cyberattacks or incidents occur. We mentioned in Play 1 that cybersecurity performance tracking is required by many regulations, including FISMA and federal CAP goals. As a result, there are also many standard monitoring mechanisms in place to help agencies report on those goals. Most notably, the Department of Homeland Security has created an entire Continuous Diagnostics and Mitigation program that helps federal agencies acquire the tools, data and knowledge to monitor their systems in real time.

However, cybersecurity performance tracking shouldn't just be a back-office task for your data scientists. It should be a public undertaking that consistently informs personnel of agency progress and how they contributed to it.

For instance, Kirschbaum said GAO often sends phishing emails to employees to determine whether their training to detect spam is sticking. GAO then reports back to personnel on how many clicked the email. But rather than making these punitive conversations, the department uses them as teaching opportunities to explain how staff might avoid similar future phishing attempts.

Performance tracking is not only an opportunity to monitor progress, but an ongoing effort to engage employees in cybersecurity objectives. Make sure to celebrate successes and the tactics that contributed to those goals, and let employees know how they are affecting the agency's security posture. Additionally, use pitfalls as an opportunity for education.



Tip from a Cyber Pro

Monitor for Understanding

"We don't want to be intrusive. We're kind of passive in that we don't actively go out and get information, we just try to pull it in and look for triggers. If we have to go out, then we can be very surgical in our request to a particular office for a particular piece of data. Then we just try to look at ways to mitigate going back to that office and asking if we can have a conversation about this because it might be that some people simply aren't understanding our policies."

— Neil Carmichael, Director, Insider Threat Program, NARA

The Team

Program Managers
Relay employees' ongoing sentiment and adoption of cyber strategies

Data Scientists
Synthesize information from multiple sources to create a singular, clear view of organizationwide cybersecurity

Engineers and Developers
Highlight cybersecurity accomplishments and pre-empt setbacks to manage messaging and leverage as teaching opportunities

The Tools

Performance Dashboard
Provides a high-level, easy-to-understand view of how your entire organization's security is being maintained for internal analysis and external education

Prioritized Security Alerts
Help security staff differentiate between the "noise" of daily IT operations and incidents that require immediate remediation or personnel outreach

Talking Points

This is important because...

"we can't rely on our non-IT staff to know every security concern associated with our tools and how to correct them. We have to make it easy for them to help us secure our agency."

After investing in this tactic, our agency can expect...

"our employees to be happier with the technologies they use, even as we better secure our infrastructure and systems."

Conclusion

The goal of this playbook is to empower non-IT public servants to aid in their agencies' cybersecurity missions. However, it's equally important for leaders to realize that this is an ongoing effort. No single strategy or roadmap will consistently achieve the goals of cybersecurity without continuous scrutiny.

"Nine times out of 10, when I see a security program implemented, the leaders implement it and then they move on," said NARA's Neil Carmichael. "But you've got to follow through. And sometimes, that involves stepping to the left slightly and reconsidering. Constantly ask yourself, 'Why are you implementing this? What problem are you trying to solve?'"

Cybersecurity is a journey during which strategies must change along with on-the-ground dynamics and escalating risks. To ensure that your agency is maintaining the most effective, organizationwide cybersecurity strategy, make sure your employees — from the frontline analyst to the highest-ranking executive — are involved in the process of updating your own playbook.

About Govloop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 270,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

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

Thank you

Thank you to DLT, SolarWinds, and Fortinet Federal for their support of this valuable resource for public sector employees.

Author

Hannah Moss, Senior Editor and Project Manger

Designer

Megan Manfredi, Junior Graphic Designer

Cyber Awareness Checklist

Share this checklist with employees at your agency. If they cannot mark each of these tactics off their list, give them the appropriate contact information for your IT or cybersecurity help desk so they can be better prepared to tackle cybersecurity in their daily responsibilities.

□ I know where to find my agency's appropriate use and cybersecurity guidelines.

□ I know where to report suspicious activity, including potential phishing emails or insider threats.

□ I do not have passwords or other sensitive personal information in locations visible to others, nor have I shared that information with anyone.

□ Every device that I have connected to agency networks is securely in my possession and protected by passwords or multifactor authentication.

□ My security training is up to date and documented by my agency.

□ My access privileges are up to date and appropriate to my job function.

□ I know what to do in the event of a critical technology failure or security breach.

□ I know how to securely use all the IT systems required to do my job.

□ I am using only approved applications, software and systems on devices connected to my agency network.

□ I know the best security practices for remotely accessing my agency's networks and systems.

Cybersecurity Usability Assessment

This template is a modified version of the System Usability Scale. Use it as a quick way to assess the cybersecurity and usability of your technologies and services for non-IT professionals.

Instructions

For each question, rank the technology on a scale of 1 (strongly disagree) to 5 (strongly agree). Each question must have an answer. If a respondent feels that they cannot respond to a particular item, they should mark the center point of the scale.

After completing the evaluation, follow these steps to calculate a total score:

1. For each of the odd-numbered questions, subtract 1 from the score.
2. For each of the even-numbered questions, subtract their value from 5.
3. Take these new values and add up the total score.
4. Multiply your total score by 2.5.

Your Score

Final SUS scores have a range of 0 to 100. Based on research, an SUS score greater than 68 is above average and anything less than that is below average.

Assessment

	strongly disagree				strongly agree
1. I think that I would like to use this system frequently.	□ 1	□ 2	□ 3	□ 4	□ 5
2. I found the security measures of this system unnecessarily complex.	□ 1	□ 2	□ 3	□ 4	□ 5
3. I thought the system's security features were easy to use.	□ 1	□ 2	□ 3	□ 4	□ 5
4. I think that I would need the support of a technical person to be able to securely use this system.	□ 1	□ 2	□ 3	□ 4	□ 5
5. I found the various security measures in this system were well integrated	□ 1	□ 2	□ 3	□ 4	□ 5
6. I thought there was too much inconsistency in this system's security protocols.	□ 1	□ 2	□ 3	□ 4	□ 5
7. I would imagine that most people would learn to securely use this system very quickly.	□ 1	□ 2	□ 3	□ 4	□ 5
8. I found the system very cumbersome to securely use.	□ 1	□ 2	□ 3	□ 4	□ 5
9. I felt very confident that I was securely using this system.	□ 1	□ 2	□ 3	□ 4	□ 5
10. I needed to learn a lot of things before I could get going with this system.	□ 1	□ 2	□ 3	□ 4	□ 5

govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P (202) 407-7421
F (202) 407-7501
www.govloop.com
@GovLoop