How Government Can Embed Information Security Into IT Best Practices

MARKET TRENDS REPORT

govloop solarwinds

Introduction

It's not easy being responsible for the safety and security of government systems and data in this day and age. Public sector IT professionals are increasingly burdened by sophisticated cyberattacks, coupled with the challenge of securing systems and data amid modernization and cloud migration efforts. Things are made even more difficult by the need to train employees and contractors, so they don't unknowingly introduce vulnerabilities into government systems.

These IT teams know that cybersecurity isn't a concern that governments can take lightly because of the sensitive data they often handle. Agencies that fail to protect their data can lose the trust of their citizens, lose access to networks, and even endanger national security.

But many challenges make staying compliant and safe difficult for agencies, even for those with the most informed and robust IT teams. Increasing insider threats, reduced budgets and end users without proper security training all conspire to thwart IT professionals who are working hard to keep their agencies secure.

The truth is that security must become every agency employee's job — and it must remain top of mind for all. To move forward, agencies should fully understand how to embed information security into IT best practices and amongst all users to protect agency data, networks, and the public.

To learn how to achieve this level of security, GovLoop partnered with SolarWinds, a leader in IT security management solutions, to explore steps for improving IT security. The report includes a look at how two large federal agencies are working to implement better IT controls that are in lock step with information security.

BY THE NUMBERS

Information Security Today

25%

of IT professionals cite budget constraints as their most significant obstacle to maintaining or improving agency IT security.

Source:
SolarWinds Federal Cybersecurity Survey Report

56%

of federal IT professionals cite careless/ untrained insiders as the largest sources of security threats at federal agencies.

Source:
SolarWinds Federal Cybersecurity Survey Report

27%

of agencies reported that they have the ability to detect and investigate attempts to access large volumes of data.

Source: Federal Cybersecurity Risk Determination Report and Action Plan

"Security guidance needs to be produced internally much faster — how to take external direction and policy and provide guidance to program managers, operators, and developers. Now the solutions are being implemented with a best guess and the guidance comes next, leading to either compliance failures or the need to redo everything."

– DoD IT Director

Source:
SolarWinds Federal Cybersecurity Survey Report

43%

of CIOs across government said cyber and information security was a priority for increased technology investment.

Source: Gartner 2019 CIO Agenda Survey

49%

of agencies have the ability to detect and whitelist software running on their systems.

Source: Federal Cybersecurity Risk Determination Report and Action Plan

THE CHALLENGE

Enforcing Good Information Security Habits

In today's ever-evolving and complex IT environment, security is more critical than ever. However, with the many responsibilities IT professionals juggle daily, the most important parts of a security model can be easily overlooked.

Enforcing good information security habits across your organization can be challenging, given constraints such as budgets, time, the complexity of compliance requests, and the evolving capabilities of attackers.

Internal end users, whether they are agency employees or contractors, can also become obstacles to good security — and sometimes, unwittingly, even become insider threats.

"End users in agencies can be a really difficult factor for security in government today," noted Arthur Bradway, Senior Federal Sales Engineer at SolarWinds. "Many people bring in bad habits and poor cyberhygiene from their personal lives to their jobs in government. It's not intentional, but they expect a lot — to be constantly connected, to use any device, and to do it however they want. And security is not always top of mind for them."

Governments are also relying more on outside contractors, increasing the risk of potential threats. Contractors without the proper security training may accidentally expose, delete, or modify critical data. They also might access resources that are not necessary to do their job, or use unsecured networks and Wi-Fi, all of which increase security vulnerabilities for an agency.

There are other challenges for IT administrators, too. An increase in the number of devices and the volume of network activity can present difficulties. The growing use of cloud apps and infrastructure increases the attack vector. In addition, the challenge of implementing good cyberhygiene and training all end users across large agencies — as well as getting leadership buy-in to do so — can sometimes seem insurmountable.

How can agencies take back control and reintroduce and reimplement information security in today's age and IT environment?

THE SOLUTION: IMPLEMENTING STRONGER IT CONTROLS

Implementing stronger IT controls and compliance monitoring is the way forward for agencies.

According to respondents of the recent SolarWinds Federal Cybersecurity Survey Report, agencies with evidence of robust IT controls are more likely to possess the hallmarks of strong IT security environments.

IT controls consist of the procedures and policies that help ensure agency employees are reasonably using technologies for their intended purposes. These involve embedding security practices and conversations about good security habits within an agency's daily office environment.

Numerous factors contribute to the successful risk management of threats posed by careless insiders:

- A concerted effort to apply security best practices
- End-user security awareness training
- Intrusion detection and prevention tools
- Employee background checks
- Patching
- Network traffic encryption

"Agencies that have worked on bolstering their IT controls experience fewer threats and are able to respond more quickly to those that do occur," Bradway explained. They also enjoy more positive results when implementing IT modernization initiatives, and are ready to comply with regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Management Act (FISMA).

"Building strong IT controls requires a deep level of visibility into one's IT infrastructure, which network and application performance monitoring tools provide," Bradway said. These types of tools continuously collect data on operations and alert IT administrators about anomalies, such as lags in performance or intrusion attempts, providing constant and valuable insight into network activities.

To strengthen their IT controls, these agencies are adapting configuration and patch management, web application security, file integrity monitoring and, of course, security. High-performing agencies with strong IT controls experience fewer cyberthreats, faster response times, and more positive results from IT modernization initiatives.

BEST PRACTICES

Embedding Information Security

I. Gamify training

IT leaders should consider embedding security practices and conversations about good security habits within the daily office environment. For example, gamifying security training by using fun and engaging activities to convey an agency's position on the importance of constant vigilance can help create a lasting, effective, and deep-seated culture of security. "A lot of current training methods aren't really engaging to the end user," Bradway noted. "You spend all that time to get your users there and they don't remember anything. By making it more engaging, they'll retain more of the information."

2. Cover all your security posture bases

According to Bradway, there are several other important yet basic steps agencies can take to improve their security posture. "These include everything from regularly updating your infrastructure inventory and identifying and protecting critical assets, to creating a plan to document process changes and leveraging automated responses, when appropriate," he explained. Other steps include utilizing two-factor authentication and documenting security incident procedures and policies.

3. Leverage cybersecurity training — and make it memorable

Solid security awareness training should help your end users think twice when they get a suspicious email or download shadow software onto a device. To make trainings stand out, gamify them, as we discussed earlier; do the trainings in person when possible; and don't lecture — involve the end users to reinforce learning.

4. Invest in the right network and application performance monitoring tools

As we've noted, building strong IT controls requires a deep level of visibility into one's IT infrastructure. Network and application performance monitoring and log management tools offer this needed visibility by continuously collecting data on operations and alerting IT administrators about anomalies, such as lags in performance or intrusion attempts, providing constant and valuable insight into network activities and failed logins.

CASE STUDY

Better Security and IT at Two Federal Agencies

Creating Better IT Visibility at the Air Force

The mission of the U.S. Air Force is to fly, fight and win in air and space. Today, a new domain has been added to that mission: cyberspace. But securing Air Force equipment, airmen and data in cyberspace is difficult.

In particular, an Air Force customer faced a lack of visibility into problems that led to network performance or capacity issues, according to a SolarWinds case study developed by TechValidate. Airmen didn't have the tools to troubleshoot network problems or outages, or any awareness of server health. They had difficulty determining whether a security incident occurred and what happened during the breach. It was difficult for them to provide end-user and systems support from a central location.

The Air Force turned to SolarWinds for help, leveraging its network, application, server and storage monitoring, as well as security and compliance tools.

With the help of SolarWinds solutions, the Air Force customer was able to correlate network, server and application issues to resolve performance problems. The base improved capacity issues configuration management, system and application monitoring, and troubleshooting. The Air Force customer also was able to boost log tracking and management and improve compliance.

Improving Network Operations at the FAA

The Federal Aviation Administration (FAA) has an incredibly daunting job: to provide the safest, most efficient aerospace system in the world.

Part of this work is keeping the systems, infrastructure and data of aerospace equipment and networks secure. This is no small task considering the FAA services more than 44,000 flights and 2.7 million airline passengers across more than 29 million square miles of airspace — daily.

The FAA was facing some IT security issues, including difficulty determining whether a security incident occurred on its networks, and, if so, what happened during the breach, according to a SolarWinds case study developed by TechValidate. Inadequate automation of compliance reporting was another challenge.

To help address these issues, the FAA turned to SolarWinds and saw a return on investment in less than three months. The agency leveraged SolarWinds products to monitor network performance, resolve configuration issues and monitor server health.

By adopting SolarWinds platforms, the FAA was able to correlate network, server, and application issues to resolve performance problems. Additionally, the agency improved configuration management and log tracking and management.

HOW SOLARWINDS HELPS

SolarWinds' suite of security and network management tools can help agencies enhance their IT controls. The company's security information event management software uses logs for security and compliance; and its network management software offers continuous monitoring, audit documentation and reporting.

SolarWinds also offers the following:

- Configuration management software that reduces vulnerabilities and centralizes change management and reporting for network devices and servers
- Patch management software that centralizes updates and helps reduce vulnerability
- Device tracking, IP management and switch port management that can help respond to threats on your network

SolarWinds security solutions and continuous monitoring tools, which correspond closely to the Risk Management Framework developed by the National Institute of Standards and Technology, play a critical role helping agencies achieve with Information Security Continuous Monitoring and other government cybersecurity strategies.

Learn more: https://www.solarwinds.com/federal-government/solution/cyber-security

Conclusion

With the rapid increase of sophisticated cyberattacks and the growing possibility of insider threats, agencies cannot afford to take their information security lightly. But by taking concrete and critical steps to embed strong security into their IT processes and controls, agencies can move toward building a strong security culture.

ABOUT SOLARWINDS

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to governments including nearly every U.S. civilian agency, DoD branch, and intelligence agency, as well as a large number of state and local government, education customers. In all market areas, the SolarWinds approach is consistent --focusing exclusively on IT Pros and striving to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use and maintain while providing the power to address any IT management problem on any scale.

Learn more at solarwinds.com/government.

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 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

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

govloop

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

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop