Market Connections®
Research you can act on.

JUNE 2020

SOLARWINDS ANNUAL PUBLIC SECTOR CYBERSECURITY STUDY

Complex IT Environments Make Cybersecurity More Difficult for Federal, State, Local, and Education Organizations

In the sixth year of the SolarWinds Cybersecurity Study, complexity joins the list of obstacles to keeping government IT secure.

Executive Summary

Public sector IT professionals face many cybersecurity challenges: increasingly sophisticated cyber-attacks, the need to secure data in the midst of modernization and cloud migration efforts, complexity of new systems, and employees who unknowingly introduce vulnerabilities into government systems.

For the last six years, SolarWinds, in partnership with market research firm Market Connections®, has kept a pulse on where and how cybersecurity threats most impact federal agencies. This year, we added state and local government and education (SLED) to identify similarities and differences across segments.

The SolarWinds Cybersecurity Study examines what agencies perceive as the biggest sources of threats, as well as the consequences of breaches, obstacles to achieving security, and where organizations feel vulnerable. We also ask how program maturity and compliance requirements impact cyber initiatives and explore what organizations can do to secure IT environments.

SHARE THIS STUDY

PRESENTED BY

solarwinds government

PREPARED BY

Market Connections, Inc.
11350 Random Hills Road, Suite 800
Fairfax, VA 22030
TEL 703.378.2025
marketconnectionsinc.com

WHERE DOES IT SECURITY FIT INTO THE ORGANIZATION?

Are IT operations/infrastructure employees on the same team as IT security? This is the norm only for education organizations. Most federal respondents indicate they have separate departments for each, and public-sector, state, and local organizations are split.

When it comes to outsourcing, the majority of respondents—and significantly more so for state and local organizations—indicate their organization's IT security operations are sourced through in-house staff. More federal than other public-sector respondents use an on-site contractor. Local respondents are more likely than state to outsource to a managed service provider.

When rating the organization's IT operations/infrastructure team's working relationship with the IT security team, respondents rate efficient use of technologies the highest. Education respondents rate efficiency when working through security issues, communication, and sharing of staff higher than ratings from federal and state and local respondents.

ORGANIZATION MATURITY

Maturity varies across the public sector, and the federal audience tends to be more mature than state and local and education audiences in its IT security capabilities. Budget constraints are the most significant high-level obstacle to maintaining or improving IT security in public-sector organizations. Complexity of the environment is one of the top challenges to improving IT security, followed by adopting a Zero-Trust approach and user segmentation. Respondents note careless/untrained insiders as the greatest source of IT security threats at their organization. But overall, most feel their organization is keeping up with threats. However, only four in ten public sector respondents are very confident in their team's ability to keep up with today's evolving threats.

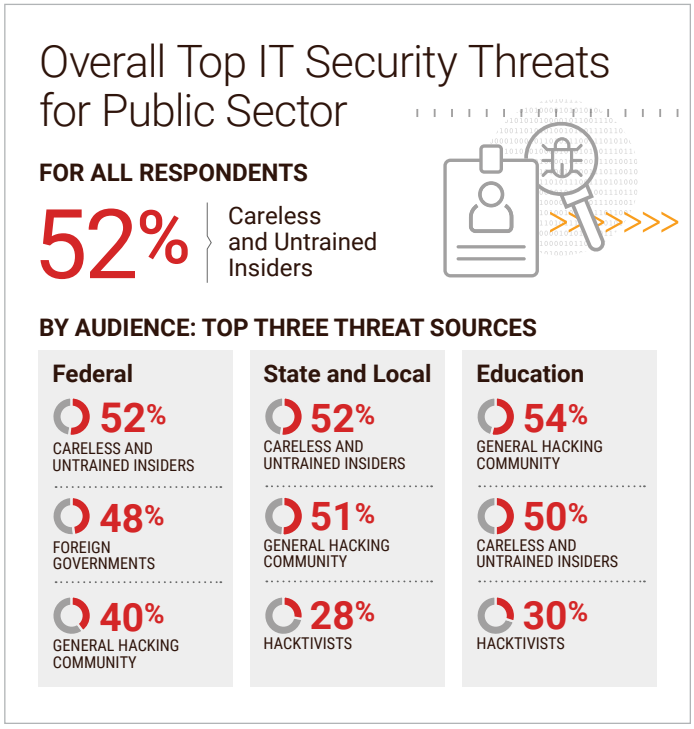
Top Survey Findings: Source of Threats

For the fifth year in a row, respondents cite careless and untrained insiders as the leading source of security threats for public sector organizations. In addition, the top three sources of security threats have remained the same for the federal audience since 2014.

Fifty-two percent of total respondents cited insiders as the top threat, a number consistent for both federal and state and local respondents. What percentage of users pose a threat, either from carelessness or malicious intent? The majority estimate only 10% or less of their organization's users are most at risk for potentially doing harm.

WHERE OUTSIDE THREATS COME FROM

The education sector cited the general hacking community (54%) as the top outside threat, perhaps in response to the string of ransomware attacks schools experienced in the last few years—well over



1,200 in 2019 alone[1]. In addition, more federal civilian organizations than defense organizations noted the general hacking community as the top threat (47%).

When compared to education respondents, federal and state and local respondents (particularly state respondents) are more concerned about foreign governments by a significant margin: 48%, 18%, and 4%, respectively. The same is true for threats from terrorists (22%, 15%, 3%, respectively). This is not surprising, as government organizations are a more likely target for this type of cyberattack.

Sixty-one percent of respondents formally segment users by risk level; however, the segmentation process is challenging for three primary reasons:

1. The growing number of systems users need access to (48%),
2. The increased number of devices (45%), and
3. The growing number of users (43%).

ACCESS RIGHTS AND ZERO-TRUST

In particular, segmenting users by risk level is a challenge for public sector organizations. Therefore, they manage the security threats both insiders and outsiders pose in the same manner.

Forty-one percent of respondents say their organization has privileged users that are not in the IT department. Yet privileged users have admin-level access to IT systems.

"Extending too much privilege across an organization can lead to increased risk," said Brandon Shopp, vice president for product strategy at SolarWinds. "A Zero-Trust strategy can offset this risk."

Nearly one-third of respondents (30%) have a formal Zero-Trust strategy in place; another 32% are modeling their approach based on Zero-Trust, but do not yet have a formal strategy. Zero-Trust security means no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources. Respondents indicate the complexity of internal environment is keeping them from easily segmenting users and adopting a Zero-Trust approach.

Top Findings: IT Security Obstacles

Not surprisingly, budget constraints top the list of significant obstacles to maintaining or improving organizational IT security.

Education respondents indicated more than other public-sector groups that budget constraints (44% in K – 12) are obstacles to maintaining or improving IT security—with their vast priorities and limited budget, security often lands lower on the list.

Approximately one-quarter of both federal and state and local respondents cited budget constraints as a top obstacle.

While budget constraints have declined since 2014 for the federal audience (40% in 2014 and 24% in 2019), respondents say the complexity of the internal environment as an obstacle that has increased (14% in 2014 and 21% in 2019).

For All Organization Types

Budget Is Top Obstacle for Maintaining or Improving IT Security

Other Top Obstacles Differ by Organization Type

FEDERAL, STATE, AND LOCAL
- Complexity of Internal Environment
- Competing Priorities and Initiatives

EDUCATION
- Lack of Training and Personnel
- Competing Priorities and Initiatives

1 Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2019." December 19, 2019. blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

The data shows this complexity is increasingly challenging, especially in federal environments where 21% of federal respondents cite it, versus 13% of state and local respondents, and 8% of education.

For federal agencies, this emerging complexity challenge may be due to the fact that, as networks have evolved over decades, they have had to combine legacy technology while scaling the enterprise across the U.S. and beyond. This can make security and compliance complicated. As education organizations typically have a flatter network involving few sites, the complexity is not a particular obstacle. State IT systems fall between the two, and thus so does their response.

Effectiveness of Tools to Foster Security

Respondents rate endpoint security software (52%) and identity and access management tools (50%) as the most highly effective security tools. It should be pointed out that respondents consider all the security tools they use to be effective, rating each tool in the survey at 80 – 90% for being moderately to highly effective.

When breaking the ratings down by organization type, more federal than other respondents indicated endpoint security software, identity and access management tools, patch management software, smart cards, and network access control solutions are highly effective at fostering network and application security at their organization.

More defense respondents (56%) than their civilian (42%) counterparts indicated that network access control solutions are highly effective. And more state than local respondents indicated identity and access management tools (state 53% and local 27%) and smart cards/common access cards for authentication (state 39% and local 17%) are effective.

A larger proportion of higher education than K – 12 respondents indicated messaging security software was effective.

Tool sprawl is a challenge when segmenting users by their level of associated risk. Almost five in ten say the growing number of systems users need access to, and 45% say an increased number of devices make segmenting users difficult.

"Not enough manpower, money, or resources. Waiting for a ticking bomb to go off." – CTO, K-12

Staying Ahead of CyberThreats

Most public-sector organizations measure the success of their IT security teams by evaluating metrics, such as the number of detected incidents (58%) or their team's ability to meet compliance goals (53%)— which, as standalone metrics, may not accurately reflect an agency's risk profile or the IT team's success. State and local respondents were also likely to consider the number of threats that were averted (56%), while education respondents focused on the level of device preparedness (46%).

Seventy-five percent of respondents indicated compliance mandates or regulations, such as GDPR, HIPAA, FISMA, RMF, DISA STIGs, etc., have had a significant or moderate impact on the evolution of their organization's IT security policies and practices. Significantly more federal respondents than other public sector respondents indicate meeting compliance goals is used to measure the success of their organization's IT security team.

OUTSOURCED VERSUS IN-HOUSE SECURITY OPERATIONS

The majority of respondents (86%) rely on in-house staff as their primary security team. Only 41% of this pool feel very confident in their team's ability to maintain the right skills. Fewer than half of public- sector respondents are very confident in their team's ability to keep up with evolving threats, regardless of whether the organization outsources its security operations.

Forty-seven percent of respondents who outsource at least part of their security operations to a managed service providers (MSP) (28% of total respondents outsource at least partly to an MSP), feel very confident in this ability.

Confidence Levels in IT Teams

for Keeping Up with Evolving Threats

LESS THAN **50%** of **ALL RESPONDENTS** are very confident in their IT security team's ability (IT security managed internally, outsourced MSP, or by in-house contractor)

For In-House IT Security Staff, Confidence to Maintain Right Skills Even Less

4 out of 10 feel very confident they maintain right skills

and **1 out of 10** are not confident at all

PROGRAM MATURITY

On average, respondents rated their organization's cybersecurity maturity at a 3.5 on a scale of one to five. They indicated that their capabilities are most mature in the following areas: endpoint protection (57%), continuity of operations (57%), and identity and access management (56%). However, there was not a single cybersecurity capability for which more than 57% of respondents claimed to be organizationally mature, which demonstrates that there is room for improvement.

Federal respondents' ratings were significantly more mature than SLED respondents in many cybersecurity capabilities. State respondents also tend to be more mature in their capabilities than local respondents. Based on this data, it appears that compliance requirements and mandates have had the most impact on organization security programs.

Recommendations: Simplify Security and Include Automation

The security landscape is continuously shifting. Even if budget constraints are removed, most cybersecurity experts struggle with finding the time necessary to stay on top of this ever-changing threat landscape. The answer is finding the right mix of tools that simplify security and automate processes. Yet acquiring the tools to keep up and accessing the expertise to implement them is often a budget issue. And to be effective, the tools need to be updated to keep current with evolving threats, which is why simplicity and automation are so important.

With the tools and processes they adopt, public-sector organizations have an opportunity to see a return on their security programs. The table below shows examples of the simple, scalable, and automated SolarWinds tools designed to address security challenges.

SECURITY CHALLENGE	PRODUCT	WHAT IT DOES
Careless and untrained insiders	Access Rights Manager (ARM)	Manages and audits access rights
	Security Event Manager (SEM)	Can see failed attempts to access restricted systems
Security threats posed by both privileged and nonprivileged users	Access Rights Manager	Helps establish and audit access privileges
Systems users need access	Access Rights Manager	Lets content/system owner approve access, as they know who should have access

SECURITY CHALLENGE	PRODUCT	WHAT IT DOES
Complexity of the internal environment	Network Performance Monitor (NPM)	Helps discover and visualize (map) complex environments
	Server & Application Monitor (SAM)	Automatically discovers and maps dependencies of application infrastructure
Address tool sprawl and confidence in system	Orion® Platform	Replaces other tools and consolidates into a single pane of glass
Evaluating metrics, such as the number of detected incidents	Network Configuration Manager (NCM) and Patch Manager	Helps eliminate known vulnerabilities and improve compliance with configuration management and patch management
	Security Event Manager	Uses logs and events to detect suspicious activities and takes automated actions
Keep up with evolving threats	SEM and NCM	Uses built-in templates to help improve compliance; NCM get updates on evolving threats from NIST® National Vulnerability Database; SEM gets updated threat feed on bad actors

Conclusions

"These results clearly demonstrate the degree to which most public-sector organizations are struggling to manage cyber-risk," said Tim Brown, vice president of security for SolarWinds.

Keeping public-sector IT secure is a herculean task for teams with limited resources—unless they have implemented strong IT controls and tools.

While the data shows a lack of organization maturity—even in technologies like endpoint protection that have been around for a long time—organizations have an opportunity to address the complexity and budget challenges they face.

One lesson the federal maturity demonstrates is compliance leads to more secure systems, and using a framework and steady improvement is essential.

The data also shows that public sector organizations can easily address the obstacles to improved security programs with budget-friendly tools. Adopting these tools can increase organizations' confidence their IT is safe and allow them to focus on other mission-critical activities.

ABOUT THE STUDY

The annual SolarWinds Cybersecurity Study is in its sixth year and—for the first time—includes state and local governments and education. The study looks at what IT decision makers perceive as the biggest threats their agencies face, the consequences of breaches, where agencies feel vulnerable, and the challenges they face in securing their agencies against cyberthreats. The 2020 blind, online survey of 400 IT decision makers included participants from federal, civilian, or independent government agencies (22%); defense (21%); federal judiciary (2%); intelligence (4%); and federal legislature (2%); state government (15%); K-12 education (13%); higher education (12%); and county government (5%).

ABOUT MARKET CONNECTIONS, INC.

Market Connections delivers actionable intelligence and insights that enable improved business performance and positioning for leading businesses, trade associations, and the public sector. The custom market research firm is a sought-after authority on preferences, perceptions, and trends among the public sector and the contractors who serve them, offering deep domain expertise in information technology and telecommunications; healthcare; and education.

For more information visit: marketconnectionsinc.com

ABOUT SOLARWINDS

SolarWinds (NYSE:SWI) is a leading provider of powerful and affordable IT infrastructure 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, and education customers. Our products give organizations worldwide, regardless of type, size or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-premises, in the cloud, or in hybrid models. We continuously engage with all types of technology professionals—IT operations professionals, DevOps professionals, and managed service providers (MSPs)—to understand the challenges they face maintaining high-performing and highly available IT infrastructures.

For more information and fully functional free trials, visit:
solarwinds.com/government or solarwinds.com/education

DOWNLOAD THE WHITE PAPER AND INFOGRAPHICS

solarwinds.com/resources/survey/solarwinds-public-sector-cybersecurity-survey-report-2020

SHARE THIS STUDY