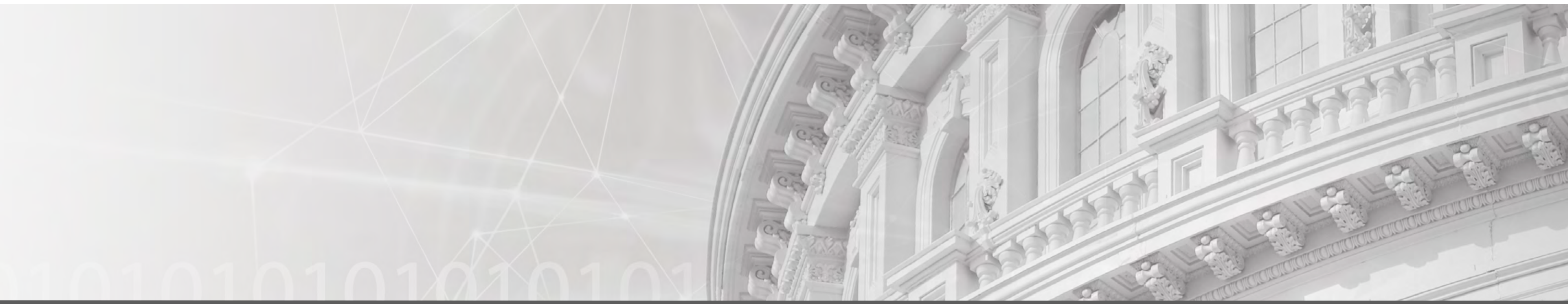


JUNE 2022

SOLARWINDS PUBLIC SECTOR CYBERSECURITY REPORT 2021

External Threats Now Lead Cybersecurity Concerns in an Evolving Landscapes

Executive Summary

To say the world has changed in the two years since we last conducted the SolarWinds Public Sector Cybersecurity Survey Report is an understatement. Everything about how we live and work has shifted—and with those shifts, public sector priorities and concerns around cybersecurity have also changed.

SolarWinds knows better than many how threats have evolved, and as a result has learned lessons that are shaping the evolution of cybersecurity in the public sector.

In this seventh edition of the study, we clearly see how the industry is changing. Once again, SolarWinds, in partnership with Market Connections, looked at where and how cybersecurity threats most impact federal and state and local governments and education (SLED) agencies.

The SolarWinds Public Sector Cybersecurity Study examines what organizations perceive as the biggest sources of threats, as well as the consequences of breaches, obstacles to achieving security, and where organizations feel vulnerable. To address the shifts over the last two years, the study also examined respondent familiarity with the Executive Order on Improving the Nation's Cybersecurity (May 12, 2021) and the perceived impact of its objectives, organizational use of a zero-trust approach and Principle of Least Privilege (PoLP) to IT, and teleworking before COVID-19, currently, and in the future.

PRESENTED BY
solarwinds government

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

SHARE THIS STUDY

Organizational Changes snd Cybersecurity Maturity

The organizational changes the public sector has made since the pandemic are as expected—employees will continue teleworking to some degree, and organizations use of a hybrid cloud approach will continue to increase.

THE SECURITY ENVIRONMENT

Before COVID-19, about half of respondents worked remotely sometimes, with close to 20% often or always doing so. Now, about two-thirds of respondents are often or always working remotely. Respondents expect that number to remain constant into the future.

In short, remote work is here to stay, which impacts the cloud strategy, particularly around security.

Organizations Host IT Security Products Across Multiple Locations

Half Prefer Cloud Locations

81%	68%	56%	52%
On-premises	Government Private Cloud	Hybrid Cloud	Public Cloud

8 out of 10 currently host products **on-premises**

Over 1/2 prefer to host products on some form of **cloud** (private/public/hybrid)

IT security products are distributed among on-premises/data center, government (private cloud), public cloud, and hybrid cloud. While the majority (81%) keep IT security products on-premises, only one-third prefer it that way. They would prefer to house IT security in some type of cloud, whether private, hybrid, or public. Currently, 68% use a government (private cloud), and 53% prefer this set up. More than half of respondents place IT security in public and hybrid clouds, and more than half prefer that location.

“What is most interesting about these numbers is that nobody is saying they’re using 100% public cloud/private cloud, on-premises or off. There is a mix, and it will likely continue to be a mix for a long time—even with the trend in repatriation we’ve seen.” said Tim Brown, SolarWinds Chief Information Security Officer. “This means having observability into all IT security tools will continue to be vital.”

ZERO TRUST AND PRINCIPLE OF LEAST PRIVILEGE

Despite the executive order (EO) and other guidance that has been issued in the last year—as well as the number of breaches happening daily—66% of respondents do NOT have a formal zero-trust strategy in place. Almost half (44%) say, though their strategy is not *forma*l, they are modeling their IT security approach on zero trust. About a quarter (23%) are not using, considering, or are not familiar with the concept.

“This is concerning,” says Brown. “As the hybrid cloud numbers demonstrate, the world is changing from on-premises, where your network consists of things between four walls, to a much broader world. In fact, whether implementing a zero-trust approach or not, we live in the zero-trust world: just look at the number of organizations that utilize Office 365 and cloud services.”

"Any more, your network is not your four walls, but all the applications you access—Azure platforms, Office 365, Salesforce, everything. Your world has gotten a lot bigger. And in this zero-trust world, decisions must be made out on the edges rather than in a central location. Zero trust is about recognizing this need," said Brown.

Part of a zero-trust strategy is adopting the PoLP, where individual users are given the minimum level of access or permissions they need to perform their job. In response to breaches and understanding the entire security footprint, respondents have been looking at PoLP more closely. The majority (80%) are somewhat-to-very familiar with it. Nearly three in ten are already implementing it, and 41% plan to in the next year, which means approximately 70% of organizations will be using it in the next year. Another quarter of respondents are considering using PoLP but not sure when they will implement it.

The Impact of
Zero-Trust Strategy

2/3 of respondents **do not** have a formal zero-trust strategy in place

AND

1 in 5 are not **currently using** or **considering** a zero-trust approach

ORGANIZATIONAL MATURITY

How protected are public sector environments? With the numbers of people now teleworking, 57% of respondents say the security posture for fully remote employees is most improved. For hybrid and onsite employees, about half of respondents rate the security posture improved over 2020 (50% and 48%, respectively).

Two-thirds of respondents say time to detection for security events has stayed the same or worsened since 2019 (52% and 59%, respectively). Respondents are also challenged with their time to respond to and resolve these events.

WHAT THESE NUMBERS MEAN

The data shows that the public sector has evolved over the last several years, but as the threat landscape changes, their challenges also evolve. The remainder of this report looks at where priorities are and the obstacles respondents face.

The Executive Order

In May of 2021, the White House issued the Executive Order on Improving the Nation's Cybersecurity. Since then, public sector agencies have been watching progress closely: the majority of respondents are familiar with the EO, with 41% being extremely familiar with it.

"The EO shows the evolution of cybersecurity, building on what we learned from the SolarWinds incident. There is a focus on improving collaboration and modernizing standards. It's solidifying how we can work better on public and private partnership perspective, how we appropriately share information, and how we become more resilient to incidents in general. That's a good thing," said Brown.

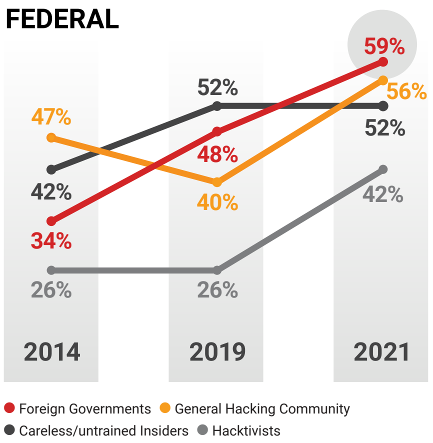
Prioritizing Executive Order Objectives

Respondents Rank All Almost Equally

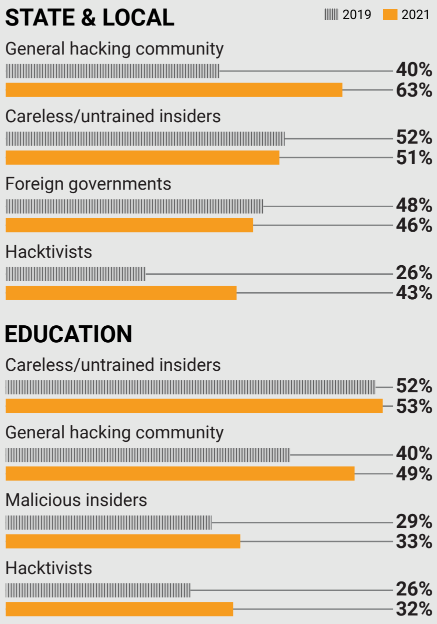
OBJECTIVE	AVG. RANK
Improve investigative and remediation capabilities	3.89
Improve barriers to sharing threat information	3.91
Create a standard playbook for cyber incident response	3.95
Improve detection of incidents on networks	4.01
Improve software supply chain security	4.03
Establish cybersecurity safety review board	4.04
Modernize and implement stronger standards	4.18

Top Concerns Over Source of Security Threats Grow and Show Major Changes

Among Federal Agencies, Foreign Governments Rise to Top while Careless Insiders are Bumped to Third



For SLED General Hacking Community and Careless/Untrained Insiders are Top Concern



Respondents were asked to rank the impact of the EO objectives. They chose improving investigative and remediation capabilities and improving barriers to sharing threat information between the government and private sectors as the most impactful, followed by creating a standard playbook for responding to cyber incidents.

Will the EO impact every facet of cybersecurity? Brown says no; cybersecurity resilience is a major work in progress for everyone. What makes the EO different, though, is that, overall, people are watching it and taking the recommendations to heart. It's about awareness, what people are thinking. It's about what they're hoping it will solve. The way respondents ranked the EO impacts align with what the study shows regarding challenges and priorities.

Top Findings: Source of Threats

When this survey was first conducted in 2014, the most pressing cybersecurity concern was insider threats based on carelessness. Concerns around careless insiders decreased by 20% this year. Instead, threats posed by the general hacking community took the number one spot, with 56% of respondents overall choosing it. However, breaking it down by respondent classification, we see that state and local governments are significantly more concerned with it, at 63%, versus 56% for federal and 49% for education. It is also a more significant concern for civilian agencies (63%) than defense (46%).

Over time, we can see the foreign aspect of cybersecurity is becoming more important. In 2014, 34% of respondents were concerned about foreign governments. In 2019, that number was 48%. Now, people are talking more about nation-state threat actors, with the SolarWinds incident and Microsoft Exchange Server data breach just two examples of the impact this growing threat presents. The data supports these discussions: 59% of federal respondents consider foreign governments the biggest source of threats for the federal government, an increase of 56% over the 2019 study.

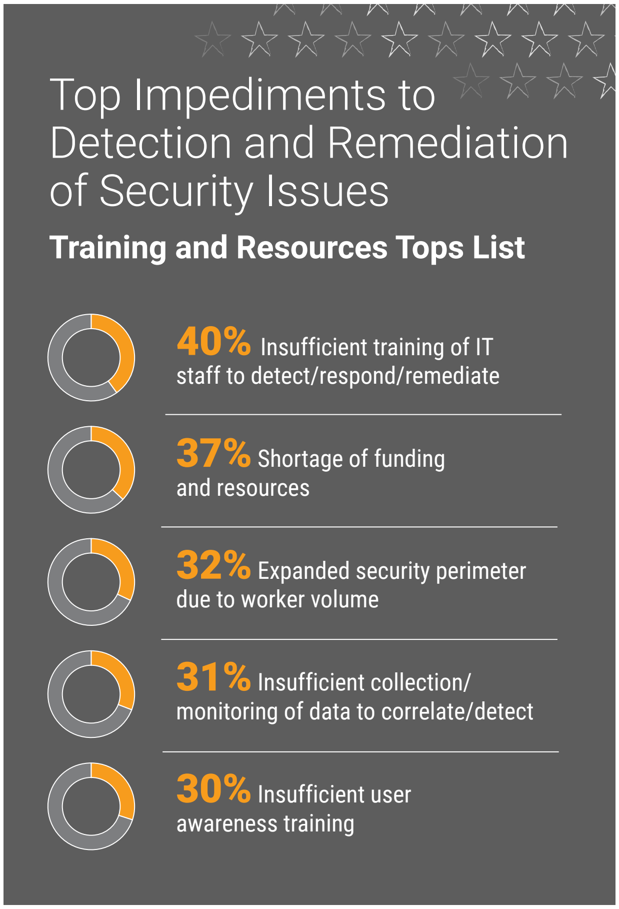
While not in the top three concerns, the hacktivist threat is something to watch. Concerns have risen significantly—42% this year versus 26% in 2019. Other threats have remained steady year over year.

Since 2019, about two-thirds of respondents note their level of concern regarding ransomware, malware, and phishing has increased. These three types of breaches are most concerning to SLED respondents.

Concerns over user permissions/credentials have largely remained the same (51%), which is interesting given the focus on identity access management (and PoLP) as the first step to a zero-trust approach and reducing cybercrime.

Top Findings: Security Obstacles

Budget always leads the list of obstacles to implementing technology, and this year is no different. Complexity of the internal environment is also a top obstacle. This year, though, it dropped from 21% to 15%, reflecting organizational maturity of cybersecurity programs.



Top Impediments to Detection and Remediation of Security Issues

Training and Resources Tops List

40% Insufficient training of IT staff to detect/respond/remediate

37% Shortage of funding and resources

32% Expanded security perimeter due to worker volume

31% Insufficient collection/ monitoring of data to correlate/detect

30% Insufficient user awareness training

Overall, the data regarding obstacles reflects the priority the public sector is, and has been, placing on cybersecurity. These low numbers do not mean, however, there are no obstacles.

The top impediments to detection and remediation of security issues focus on staffing and funding. Insufficient training of IT staff is an impediment to 40% of respondents, and 37% cite a shortage of funding and resources. One-third cite the expanded security perimeter due to the volume of remote workers and insufficient collection/monitoring of data to correlate events and detect threats as impediments.

The top four impediments align with the challenges of the remote work environment and how the network has inherently changed. Brown says they speak to the need to have monitoring tools that provide complete observability into the network.

When asked to rate the importance of a range of IT security products and solutions, respondents rate network security software highest. However, all the tools were highly rated—most in the 70th percentile. This indicates respondents know the value of various security solutions on the market. The question becomes how to implement the long list of options. While the question we asked wasn't about obstacles, the responses show that making investment decisions is, in fact, an obstacle. When everything is a priority, nothing is.

Top Findings: Investment Priorities

Respondents have a range of investment priorities to address their cybersecurity challenges and goals. IT security priorities lead with intrusion detection and prevention (68%), access management (67%), and vulnerability management (65%)—a direct response to the nature and severity of cyber breaches over the last few years. Infrastructure investments lead with remote access capabilities, collaboration tools, and improved troubleshooting capabilities, all of which will facilitate observability into what is happening on the network.

These priorities align with how environments are evolving. With environments moving beyond the on-premises world, monitoring activity and troubleshooting become harder. For example, it is extremely challenging to identify and fix issues in a hybrid environment because some apps are running in a cloud and some on-premises. Finding the root of any single problem hinges on being able to observe what is happening across the entire ecosystem. The greater use

Are Constantly Changing Requirements Creating a **Prioritization Bottleneck?**

IT SECURITY	
Intrusion detection and prevention	68%
Access management	67%
Vulnerability management	65%
Security event and incident management	65%
Improve compliance	65%
Education and training	63%
Implementing zero-trust framework	61%

INFRASTRUCTURE	
Remote access capabilities	62%
Collaboration tools	61%
Improve troubleshooting	59%
Remote support tools	59%
Network core	58%
Capacity planning and optimization	58%
Disaster preparedness	58%

MODERNIZATION	
Replace legacy applications	60%
Migrate systems to cloud	60%
Virtualize/consolidate data center	59%
Utilize digital services	59%

of Software as a Service (SaaS) means that previous methods of troubleshooting no longer work.

The bottom line is a strong security posture requires more visibility, tracking, tracing, metrics, and data across the environment.

Modernization priorities are also important. Agencies need to replace legacy applications (60%) and migrate systems to the cloud (60%). Customer experience and digital transformation are slightly lower priorities but still have more than half of respondents prioritizing them and therefore remain important.

The study broke out IT service management (ITSM) and application performance monitoring (APM). APM is a high priority from a customer experience investment perspective, which is interesting. Where ITSM touches users everywhere, APM tends to touch only the IT professional only. Brown says the importance of customer experience in APM is important because the IT professionals aren't getting the full picture they need to do their job. They need better tools.

The digital transformation priorities listed point to the hybrid world. When transforming from a four-walled environment to a much larger network, the network is essentially everything. Brown says when you need to have a stakeholder platform or a portal, it means you want visibility across the entire environment—not just visibility into one section of it. The priority for database infrastructure again supports the need for a single viewpoint for database models.

Recommendations

One of the biggest takeaways from the study is that everything is a priority. The problem is, even with an unlimited budget and staff resources, prioritizing everything is not possible. Based on lessons learned from recent breaches and the EO, SolarWinds recommends turning lessons learned into actionable insights that can effectively drive change:

- It's important to understand your environment.
- It's important to have visibility into your environment.
- It's important to have knowledge about your environment.
- It's important to start with a baseline, and that baseline starts with visibility across your environment.

"When the breach happened, we discovered a hole that made us rethink, relook, and reconsider our entire approach. We've had the opportunity to revamp all of our processes, and now we can give more knowledge and more information," said Brown.

Having observability into your environment is key. That does not necessarily mean making new investments though. The first step is to conduct an environmental audit so that you can see how to secure your unique systems in a specific way, based on what is most important to your organization, customers, and users.

That means you need to know what your mission and business critical assets are. You need to know what is going to affect you the most. You need to know what's most important in your environment. Most of the IT security solutions are very important, but only in as much as they map to ultimate goals.

Conclusion

The 2021 study showed that the public sector is maturing and evolving. In many ways, the extreme events of the last two years have propelled that evolution forward. The obstacles of two, three, and five years ago are no longer obstacles—and that's a good thing for the public sector. The changes are improving cybersecurity and collaboration. The public sector is becoming more resilient to incidents in general. But in this rapidly changing world, prioritizing next steps can still be a challenge. The good news is that tools, processes, and guidance exist to help you work through it in the most effective way for your agency.

ABOUT THE STUDY

The annual SolarWinds Cybersecurity Study is in its seventh year. The study looks at what IT decision makers in federal and state and local governments and education 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 2021 blind online survey of 400 IT decision makers included participants from federal, civilian, or independent government agencies (29%); defense (18%); federal judiciary (1%); intelligence (2%); federal legislature (1%); state government (10%); K–12 education (13%); higher education (13%); city/municipal government (7%); and county government (8%).

ABOUT SOLARWINDS

SolarWinds (NYSE:SWI) is a leading provider of simple, powerful, and secure IT management software. Our solutions give organizations worldwide—including nearly every U.S. civilian agency, DoD branch, and intelligence agency, as well as a large number of state and local governments and education customers—the power to accelerate organizational transformation in today's hybrid IT environments. We continuously engage with technology professionals—IT service and operations professionals, DevOps and SecOps professionals, and database administrators—to understand the challenges they face in maintaining high-performing and highly available IT infrastructures, applications, and environments. The insights we gain from them, in places like our THWACK community, allow us to address customers' needs now and in the future. Our focus on the user and commitment to excellence in end-to-end hybrid IT management have established SolarWinds as a worldwide leader in solutions for observability, IT service management, application performance, and database management.

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

ABOUT MARKET CONNECTIONS, INC.

Market Connections, a portfolio platform of GovExec, 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

DOWNLOAD THE WHITE PAPER AND INFOGRAPHICS

Visit this link to download the full report.

SHARE THIS STUDY