How to Support Multiple Work Styles

Cybersecurity Best Practices for You and Your Agency

RESEARCH BRIEF

govloop citrix

Introduction

During the past 20 months, agencies reached a point where they knew returning to a pre-pandemic world wasn't going to happen. Now, they are grappling with the pandemic's long-term outcomes, making on-the-ground action plans around remote work and cybersecurity for the abiding resilience of their organizations.

The reality they face is that the surge in remote work solidified the diversity of work styles they now need to secure. In other words, employees often work and access IT resources differently when they're in the office vs. remote, at home or on the go. Agencies not only need to secure these varying work arrangements, but also allow their employees to work productively at the same time.

To learn how organizations are approaching this challenge, GovLoop partnered with Citrix, a leader in digital workspace solutions, to produce this report. We surveyed employees with varying backgrounds across federal, state and local governments to get a wide-ranging sense of cybersecurity concerns, initiatives and attitudes in government organizations.

In this report, we address four main questions:

+ **How concerned are leaders about cybersecurity?**
+ **What is the impact of remote work?**
+ **How invested are employees in their agencies' cyber posture?**
+ **Exactly how widespread is zero trust, the favored security framework in government?**

Note: Charts may not add up to 100 due to rounding.

Who We Surveyed

We surveyed 86 respondents in August 2021.

FIGURE 1

I work for...

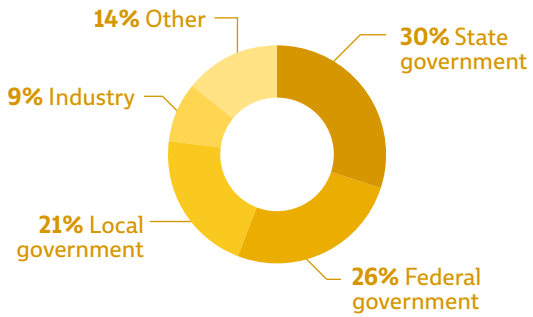
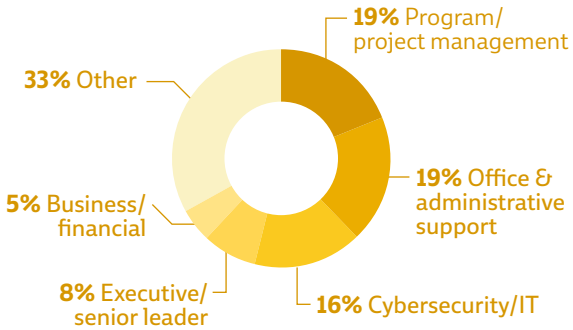


FIGURE 2

Which of the following best describes your area of expertise?

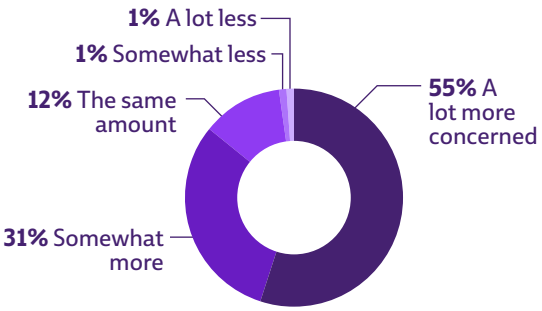


Leadership Concerns

The numbers don't lie: Cybersecurity is an increasing concern for government leaders. The majority of respondents (86%) said their leaders have become somewhat or a lot more concerned about cyberthreats in the past two years (see Figure 3).

FIGURE 3

Over the past two years, have your organization's leaders become more or less concerned about cyberthreats affecting your agency?



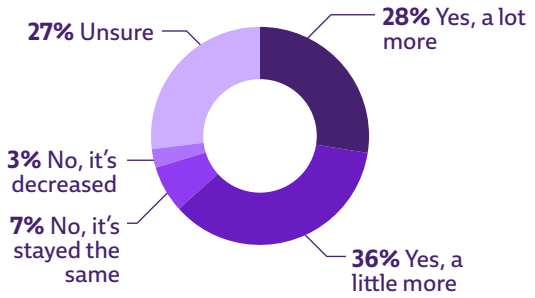
This isn't surprising, especially because of the quick expansion of remote work.

"The attack surface of an individual agency or organization has expanded significantly," said David Smith, Managing Director of State and Local Government Sales at Citrix. "There was a lot more control of who was accessing what from where and how prior to the pandemic. **With remote work — and what is going to turn into hybrid work — it has become a bit more challenging from an IT perspective, and opened the door for malicious actors to try to work their way into an organization."**

The concern is palpable in agencies' spending. It's not just talk when it comes to leaders' worries. More than half of respondents said they saw cyber spending increase in the past two years (see Figure 4), meaning as concerns increased, spending did too. Despite the fact that budgets are limited — especially in state and local agencies — they are choosing to invest in cybersecurity.

FIGURE 4

Has your agency increased spending on cybersecurity (patches, training, backup, security solutions, etc.) in the last two years?



Still, cybersecurity remains just a fraction of the budget for state governments. A 2020 report from the National Association of State Chief Information Officers (NASCIO) found that insufficient cybersecurity funds is the No. 1 barrier to cybersecurity challenges. Most states allocate just 3% of their total IT budget to cybersecurity.

> ***"We believe that a dedicated cyber program funding — even when assigned as part of the overall IT budget — can help state CISOs [chief information security officers] and CIOs give the state legislature and executive branch leaders the right level of visibility into state cybersecurity spend in an effort to raise funding levels."***
>
> ***- NASCIO***

What to Look for in the Security Market

If spending is increasing, government agencies are likely shopping around for security tools. Smith shared some best practices on what agencies should look for in top-tier solutions.

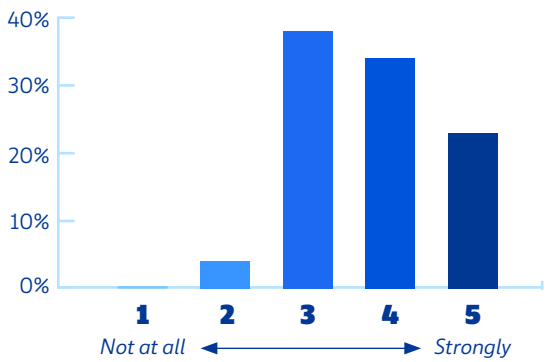
Look at tools that rely on understanding the context of the user, meaning users' locations, the type of application they're accessing, what device they're using and how they're using it. Adjust security based on context.

Consider how you can make it easier for the user to work while maintaining security. Employees work differently in the office vs. from home. When agency operations can't securely accommodate multiple work styles, employees inevitably find workarounds to remain productive. This leads them to do things they shouldn't, such as using an unsanctioned email application instead of an approved one. Reduce the temptation by providing productivity-friendly cyber solutions.

Bring the user to the data and applications, instead of the data and applications to the user. This way, you can maintain high-level security for your most important assets and give users access to only the things they need, rather than everything. You can have more control in that scenario, especially in remote work.

FIGURE 5

On a scale of 1-5, to what extent is the experience of remote work leading to changes in your agency's modernization and security strategies?



Remote Work's Impact

Sometimes cybersecurity can go unnoticed by workers who don't specialize in cybersecurity or aren't directly involved in cyber efforts. But remote work left an impression big enough for employees to notice. The median score respondents chose for the impact of remote work on security was 4, with 5 indicating the strongest impact. Additionally, no one said that remote work had zero effect on security strategies (see Figure 5).

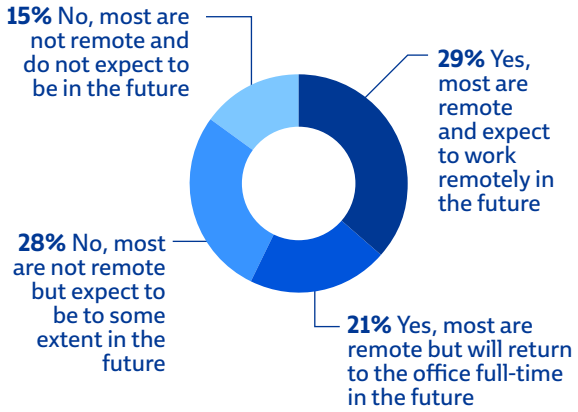
As Smith said earlier, agencies' potential attack surface widened when the workforce dispersed and new networks, devices and endpoints appeared. The traditional security framework, which was already becoming outdated, became even more unsuitable for the distributed government workplace.

Most employees don't plan to return to the old way of working. Eighty-six percent of survey respondents are working remotely now or expect to in the future to some extent (see Figure 6). The majority of respondents (80%) also said their organization deployed new cyber tools during remote work (see Figure 7). This means agencies must contend with increased complexity of their cybersecurity stack.

As agencies begin to open office doors and roll out return-to-work strategies, they need to address the complexities of the hybrid environment and employees' various work styles.

FIGURE 6

Is your organization working remotely now?



Best Practices for Securing a Hybrid Workforce

In the long term, remote and in-person work is here to stay. In this new environment, how can agencies secure their end users?

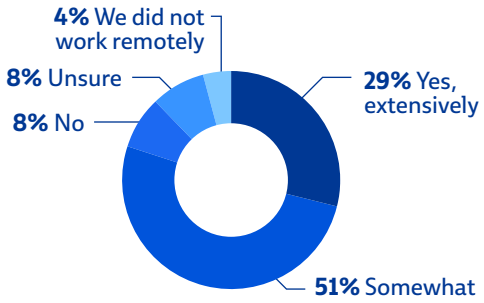
Eliminate confusion and complexity. Start by clearly identifying the best ways to work in different environments. It's difficult to train people to do their jobs differently in the office vs. remotely or on the go vs. at home. "Eliminating end-user complexity is one of the things organizations can do to make sure their users are protected," Smith said.

Eliminate multiple points of access. If employees have three or four entry points to applications and data, malicious actors also have these entry points. Maintaining a strategy that gives you control over the point of access is important. Single sign-on (SSO) gateways allow centralized control of authentication policies, and multifactor authentication (MFA) helps double-check a user's identity when they're accessing applications and data.

Adopt adaptive security. "IT can't be a yes/no decision," Smith said. Just because an employee is not on a government network or a government-furnished device doesn't mean they should not be productive. Security should adapt to users' context. Let's say a remote employee's work laptop crashes and they have only a personal device on hand. Adaptive security allows them to keep working with certain available capabilities or assets, such as view-only documents, while other capabilities, such as saving files locally, are accessible only on trusted devices.

FIGURE 7

While employees worked remotely during the pandemic, did your organization deploy new cybersecurity tools or capabilities?



Securing Data and Applications, Too

Employees aren't the only ones working in varying environments.

"Users have become more dispersed, and applications have become more dispersed," Smith said.

Data and applications no longer just sit in data centers. Like remote workers, they're distributed throughout different locations, such as private and public clouds and on-premise sites.

That means there are more targets for cyberthreats other than end users – things like devices, networks, individual applications and application programming interfaces (APIs), which are intermediaries that allow multiple applications to interact with one another. There are ways to protect each area, but agencies must have a comprehensive, high-level plan around defining the most important data and applications, and how users will interact with them to allow productivity and maintain security.

Employee Influence

IT and cybersecurity leaders understand that individual employees play an important role in keeping agencies secure. But how well do employees know this? According to the survey, very well. On a scale of 1 to 5,the median score of how much respondents believed they impacted their agency's cyber posture as individuals was 4, with 5 being the highest score (see Figure 8).

Local government respondents believed this most, with 46% scoring 5. Forty-one percent of state respondents and 23% of federal respondents believed the same (see Figure 8). This makes sense given the size of each level of government. Local agencies tend to be smaller than state and federal governments, so staff may feel a greater share of responsibility for the security of their organization. Recent ransomware attacks targeting local governments may contribute to this feeling, too.

Strong awareness may also mean that organizations' security training is paying off. "With the increase in training, I think people are realizing more that they are a critical element in the overall cyber ability of an organization," Smith said.

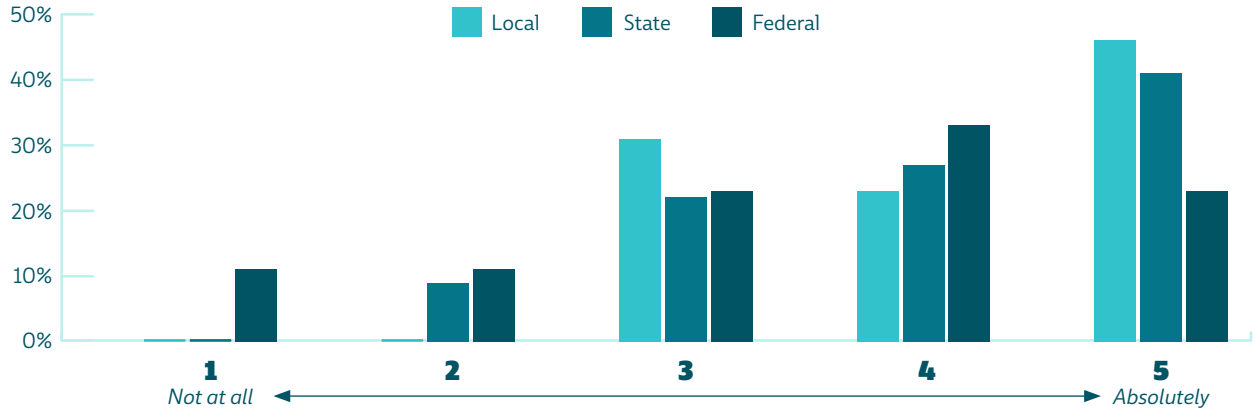
It also may have to do with the fact that they are dealing with cyber concerns in their personal lives. Many have probably received a notification about a data breach or read the news about a leak. "People are more used to understanding that these things can happen, and thus understand the important role of individuals," Smith said.

How Employees Can Secure Their Organizations

"If you see something, say something," Smith said. Flex your security training muscles. Be aware of suspicious or random emails and phone calls. Malicious actors can sound legitimate, using information such as real names and titles from social media to target you.

FIGURE 8

To what extent do you believe that you, individually, affect your agency's cybersecurity posture?



Zero Trust as the New Cyber Lifestyle

President Biden's executive order has signaled that zero trust will be the future of cybersecurity.

In September 2021, one-third of projects supported by the Technology Modernization Fund (TMF) – a grants vehicle for federal IT modernization – focused on zero trust implementation. Zero trust architectures are dynamic and adaptable enough to tackle both the IT needs of the hybrid workforce and cybersecurity concerns.

"The technologies that used to be dominant in the areas of remote access don't necessarily apply well to the types of applications and work scenarios users have today," Smith said.

Some of those technologies are virtual-private networks, which encrypt a device's connection to an internal network like a tunnel. They complicate secure access to IT resources because they were originally designed for traditional "castle-and-moat" perimeters, or cybersecurity for a physical location. They don't work as well in the hybrid work environment, where users and data are dispersed.

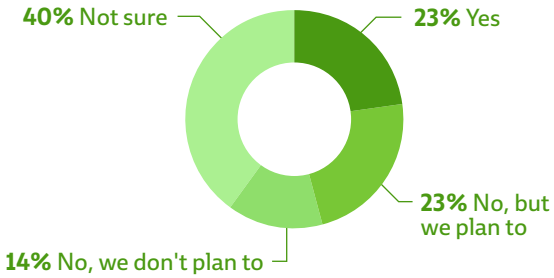
As such, zero trust became the signature cybersecurity model of the pandemic. It allows the new security boundary to be the user, not a limited location, such as a building or network. And it allows agencies to make better, more contextual and more informed security decisions than before.

Although 46% of respondents said their agency has implemented or plans to implement zero trust, 40% said they're unsure. Fourteen percent said their organization doesn't plan to implement it at all (see Figure 9).

"One reason why people may not be going down this zero-trust direction is that it is an area that's still evolving," Smith said. "A lot of organizations are still trying to understand zero trust and exactly what it means to implement a zero-trust approach." Agencies also don't always refer to zero-trust architectures as "zero trust."

FIGURE 9

Has your agency implemented zero trust security?



Zero Trust: A Quick Refresher

Most agencies rely on perimeter-based security, which is commonly compared to a castle and moat. It works like this:

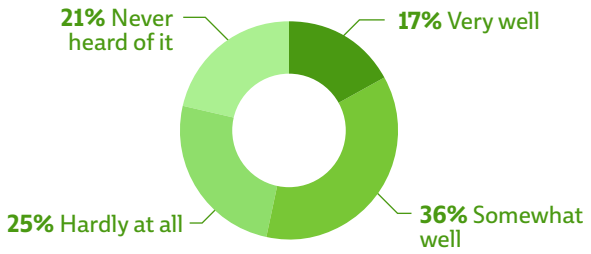
- A security guard is posted on one side of the moat and can lower a drawbridge to allow entry.
- The guard questions everyone who seeks entry. That is, the guard checks the identity of individuals and their reason for entering the castle.
- Once granted entry, however, people have free range around the castle grounds. In short, everyone who makes it past the guard at the moat is considered trustworthy.

In zero trust, that guard is just the first line of defense. Guards are also posted outside key rooms throughout the castle, checking the identity of visitors and whether they have permission to access the room in question.

Our survey found that 25% of respondents hardly understand the basics of zero trust, and 21% never heard of it (see Figure 10).

FIGURE 10

How well do you understand the basics of zero trust security?



To help agencies that are using zero trust for the first time, Smith outlined some principles to consider.

Principles for Implementing Zero Trust

A strong identity authentication foundation. You need to consistently identify a user across applications.

A technology stack that integrates across applications and services. Throughout the diversity of applications that organizations are delivering, from cloud-based applications to third-party services, you must have a technology presence that integrates with all of them.

How Citrix Helps

Citrix works with customers to provide an effective and secure workspace solution for all work styles – wherever an application lives and whatever the user scenario is.

Through solutions such as virtualization, it allows user access to applications and desktops that run in an organization's data center or the cloud while keeping data secure. It provides MFA and SSO capabilities with adaptability, so IT can enable and disable access based on user context. And through tools such as Secure Internet Access and Secure Browser Service, it supports user productivity without putting organizations at risk. Citrix allows users to access any kind of data or application over any network, via any device, regardless of the type of work that needs to get done.

Conclusion

Agencies are in the thick of building the new government workplace in a more secure and dynamic way. The hybrid environment, in which people are working in offices, at home and even on the go, has changed how they approach cybersecurity.

Our survey found that leaders are more concerned about cyberthreats than in the past. Remote work has also introduced many complexities in work styles, tools and cyber strategies.

But the good news is twofold: Zero trust is here to simplify complexities and create a more secure path forward. And employees are here for the ride, more invested in their organizations' cybersecurity journey than ever before.

About Citrix

Citrix (NASDAQ:CTXS) aims to power a world where people, organizations and things are securely connected and accessible to make the extraordinary possible. Its technology makes the world's apps and data secure and easy to access, empowering people to work anywhere and at any time. Citrix provides a complete and integrated portfolio of Workspace-as-a-Service, application delivery, virtualization, mobility, network delivery and file sharing solutions that enables IT to ensure critical systems are securely available to users via the cloud or on-premise and across any device or platform. With annual revenue in 2015 of $3.28 billion, Citrix solutions are in use by more than 400,000 organizations and over 100 million users globally.

Learn more at www.citrix.com/government.

About GovLoop

GovLoop's mission is 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 the public sector.

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

govloop.com | ***@govloop***