How Agencies Are Redrawing the Cyber Roadmap

citrix™ govloop

One year of remote work did not create new security problems for agencies. Instead, the experience highlighted security challenges that were already there.

That was a common theme throughout GovLoop's Briefing Center, "Ramping Up for the Future of Gov — Why Cyber Needs to Change," an online training during which government and industry experts shared their experiences and insights around how agencies can improve their cyber defenses.

For example, several speakers discussed how remote work has demonstrated the potential value of a zero trust-based approach to cybersecurity, with its shift away from a perimeter-based security (see story, p. X). But cloud computing, mobility and other technologies were already undermining perimeter security years before the pandemic.

Likewise, the challenge of supporting a large number of remote workers has driven home the importance of ensuring that security solutions and policies fit with how users work, rather than becoming obstacles that they try to work around.

But the pandemic was not only a security challenge. Recent months have brought several high-profile security breaches that caught government agencies off guard and highlighted key issues that need to be addressed.

In short, agencies everywhere have an opportunity to use the lessons learned during the pandemic to push for changes that will benefit them for years to come.

"Some of the recent breaches and events that have happened in the world around us have only put an exclamation point on the need for really implementing a new security model," said keynote speaker Tony Scott, Former Federal Chief Information Officer and now Chairman of the Tony Scott Group.

This briefing distills some of those lessons learned. To dig deeper, be sure to check out the on-demand version of the Briefing Center.

Watch the recording: "Ramping Up for the Future of Gov — Why Cyber Needs to Change"

Experts

Alma R. Cole

Chief Information Security Officer and Executive Director, Cybersecurity Directorate, Office of Information and Technology, US Customs and Border Protection, Department of Homeland Security

Jeremiah Cunningham

Vice President, Federal, Citrix

Chris McMasters

Chief Information Officer, city of Corona

Corona Ngatuvai

Enterprise Architect, state of Utah

Gary Pentecost

CTO, Public Sector, Citrix

Tony Scott

Former Federal CIO, Chairman of the Tony Scott Group

Zero Trust: A Primer

As some cybersecurity experts see it, remote work is a perfect use case for a zero-trust approach to cybersecurity.

Zero trust architecture originally emerged more than 10 years ago in response to the proliferation of cloud computing, mobility and other technologies that extended applications and data outside the network perimeter. Experts said that with the network perimeter becoming more porous, organizations needed to apply security controls at the application and data levels.

With remote work, the perimeter has been more porous than ever, and the benefits of zero trust have become clearer. Experts believe that the experience of the last year will lead to a surge of interest in zero trust.

But what is zero trust? Think about security for an office building.

In most government buildings, you need to show your pass or use your fob to get past the lobby. That's perimeter-based security.

But that doesn't mean that you have access to every office within the building. Instead, your manager probably let the security office know which offices or meeting rooms you need to access. Each time you need to access one of those rooms, you need to use your fob again. That's zero-trust security.

In short (and simplified form), with zero-trust architecture, every time you attempt to access a network resource, the network will do three things:

- Authenticate your identity
- Check the security status of your device
- Verify that you have permission to access that resource.

Tony Scott, Former Federal CIO and now Chairman of the Tony Scott Group, said that the complexity of the IT environment necessitates a new approach. Agencies need to think more carefully about which resources individual users need to access.

"[It's like] even in an office building, we have access to a lot more than we realize or maybe should be allowed to have access to," he said. "So, the concept of zero trust is a 'less is good' sort of model."

Zero Trust Guidance

For organizations looking to move to zero trust, help is on the way.

The National Security Agency recently published a report titled "Embracing a Zero Trust Security Model," which discusses both the benefits and challenges of a zero trust architecture and provides recommendations on how to implement it (see sidebar).

Meanwhile, the National Institute of Standards and Technology is developing guidance for applying a zero trust security model to address six common challenges across agencies, from employees needing to access network resources to cross-enterprise collaboration with partner organizations.

Zero Trust in a Nutshell

As part of its report, NSA has identified three guiding principles of zero trust:

1. **Never trust, always verify.** Treat every user, device, application/ workload, and data flow as untrusted. Authenticate and explicitly authorize each to the least privilege required using dynamic security policies.
2. **Assume breach.** Consciously operate and defend resources with the assumption that an adversary already has presence within the environment. Deny by default and heavily scrutinize all users, devices, data flows, and requests for access. Log, inspect, and continuously monitor all configuration changes, resource accesses, and network traffic for suspicious activity.
3. **Verify explicitly.** Access to all resources should be conducted in a consistent and secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access decisions to resources.

A User-Centric View of Cybersecurity

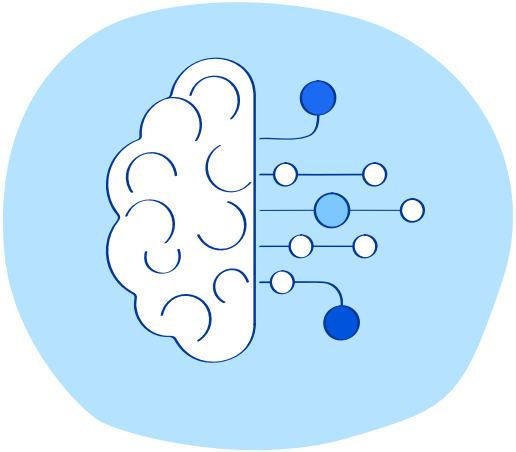
We've all been told what we can't do on our employer's computer networks. We're regularly reminded what websites we shouldn't access and what free software tools we can't download from the internet — even if they make our jobs easier.

It's all for good reason, but cybersecurity can often feel restrictive and at odds with the very mission government employees signed on to do, such as public education, grant management, health care services, fire and rescue and a host of other services.

But the large-scale move to remote work, combined with recent high-profile cybersecurity attacks have forced government agencies to rethink how they invest in and implement cybersecurity practices that are effective yet also user-friendly.

That was a common theme throughout the Briefing Center. Experts from government and industry shared their cybersecurity priorities, how these changes impact employees and the way they work and why it's critical for agencies to balance security and usability.

Here we've included a roundup of takeaways from each speaker.



COVID-19 Accelerates New Security Models

In a telework environment, a change to the security posture is needed, said Scott.

As opposed to walled cybersecurity with a soft underbelly, identity and access must be hardened and verified constantly. Scott described it as a whitelist — devices and accounts that are allowed — versus a blacklist — devices that aren't.

Scott identified automation and education as two areas where agencies can improve immediately, moving toward modern security without "boiling the ocean."

Automation can fill gaps in the cyber skills shortage. And agencies can look toward the Girl Scouts — yes, the Girl Scouts — as a model for cybersecurity education and engagement.

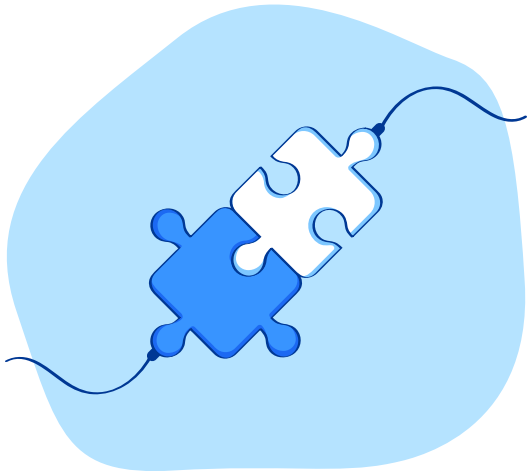
Security as an Enabler

Chris McMasters, CIO for the city of Corona, is a security shop of one. As such, he is a firm believer that all city employees play a role in cybersecurity.

As he puts it, "everyone in some shape or form is a cybersecurity professional."

He involves employees in security conversations about top threats and helps them understand the role they play in keeping data, systems and the mission safe.

He sees his role as an enabler, to support the business of government and ensure people can work in a way that's most conducive to them. Using gamification, infographics and short digests, he's proven that security and usability need not be at odds.



Balancing the Basics With Newer Tech

Corona Ngatuvai, Enterprise Architect for the state of Utah, and his team see artificial intelligence and machine learning as critical for making decisions faster, identifying anomalies and ensuring employees can securely access what they need.

But these investments don't negate security basics. You can't assume that everyone knows what a phishing email looks like just because they passed the annual exam, he said.

One measure of success is how many employees fall victim to phishing simulations and whether education helps or if further actions must be taken.

"We train you to keep you safe," he said. "If we can't keep you safe, we have to look at other things."

Zero Trust: A Logical Solution

Remote work — and the likely emergence of a post-pandemic hybrid work environment — is pushing agencies toward a zero trust architecture, said Gary Pentecost, Networking Director of Sales Engineering for the U.S. Public Sector at Citrix.

With the increasing mobility of the workforce, agencies can't think about security in terms of on premises versus remote. "We need to create solutions in ways that allow users to access what they need, when they need it, wherever they are working," he said.

Because zero trust puts security controls around individual network resources (e.g., applications and data), it provides a cohesive approach to supporting that hybrid environment.

User Experience Key to Security

Indeed, the user experience is a vital concern when it comes to security, said Jeremiah Cunningham, Senior Director for Federal Sales at Citrix.

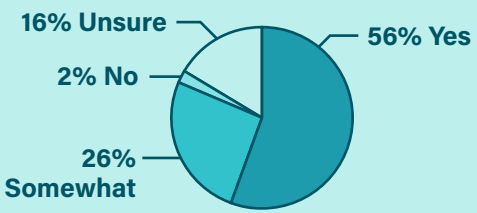
"It used to be that you gave up a lot of performance to get security," he said. "Now, we want performance, but we also want security, and the move to the cloud is driving that."

In the past, people working remotely typically had to use a VPN, and they took it for granted that performance would suffer. But that's not the case with cloud solutions. These days, people expect the same experience, no matter where they are working or what devices they are using, Cunningham said.

Change is Afoot in Cybersecurity

As part of the Briefing Center, GovLoop asked attendees whether their agency's security posture had changed in the last year — the last year, of course, being the year of remote work.

Has your agency's security posture changed in the last year?



More than 80% of attendees said security had changed or changed somewhat. This is encouraging, said Scott, because it means that agencies have recognized the need to adapt to changing circumstances.

"I think out of necessity most organizations have had to react to both work from home and some of these other challenges that have presented themselves. I would interpret the results of that as good," he said.

This is also good news for employees who just want to get their work done, said Ngatuvai.

"In my mind, it's kudos to your security folks if they're implementing these changes and you're oblivious to it, so that you can focus primarily on being productive," he said.

3 Lessons from the Recent Cyberattacks

Two recent cyberattacks demonstrate why government employees can be lax about cybersecurity.

Agencies using SolarWinds software were breached in 2020, and governments leveraging Microsoft tools were impacted in 2021. Both incidents left multiple agencies facing negative publicity, disappointed citizens and costly post-incident investigations.

Yet every misstep also creates room for improvement. Nationwide, agencies are now debating how to avoid these types of crises.

"The adversaries are going to get through, so you need to ensure you have the ability to detect and to respond," said CBP's Cole.

Cole shared three lessons agencies can learn from the Microsoft and SolarWinds breaches to strengthen their cybersecurity.

1. Emphasize Education

The reality is that employees are not always in sync on cybersecurity. To reduce internal confusion, Cole recommended agencies familiarize their staff with clear cybersecurity principles.

"The first lesson that you have to drive home to all of your stakeholders is the Cybersecurity Framework," Cole said.

2. Carefully Vet Products and Vendors

Criminals will exploit people and products that do not keep up with cybersecurity developments. Consequently, agencies should choose potential private-sector partners wisely before adopting new technology.

"As you open yourself up to those technologies, or those partners, or bring those technologies onto your network, now you're exposing yourself to some of the risks that they may have that are left over," Cole said.

3. Scrutinize the Supply Chains

Technology supply chains are increasingly a concern for agencies. According to Cole, these systems can create risks for agencies.

"It might be easier for them to go break into one of your partner networks, a vendor or something else, and embed themselves there instead of going for that frontal assault," Cole said of cybercriminals.

Using breaches like the Microsoft or SolarWinds ones as guides, agencies can better prepare for future threats.

Top Cybersecurity Questions Answered

As part of the government panel, each speaker was asked to share the most common cyber-related question that they get from agency employees. Here are the questions and the gist of the answers provided.

Q: "Is it OK for us to use this?"

"Everybody wants to be as productive as they can be, for as low a cost as possible. With a lot of these [Software-as-a-Service] products, people can try something for free and then get hooked on it.

This is challenging for us to manage because we want you to be productive — we can see how that tool facilitates being more efficient. But we don't know where the data you're putting into that system goes. Those are things we need to be smarter about."

– Corona Ngatuvai, Enterprise Architect, state of Utah

Q: "Why is this website blocked?"

"Security exists to support organizations. They're not there for security's sake. It's a way to make sure that we can accommodate all the business flows and make sure everyone can run what they need to run — but while still ensuring that we are securing both our systems and the public's data."

– Alma Cole, CISO & Executive Director, Cybersecurity Directorate, Office of Information and Technology, U.S. CBP

Q: "Is the organization secure? Am I cybersafe?"

"Everyone, in some shape or form, is a cybersecurity professional. So we work on educating them, we work on giving them an understanding of what the top threats of the day are, for instance, and making sure that that gets pushed down to the organization."

– Chris McMasters, CIO, city of Corona

How Citrix Helps

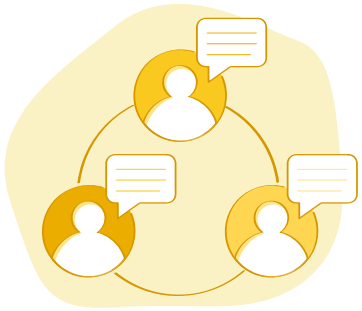
Citrix provides workspace technology that is designed to deliver a frictionless employee experience — with a common set of capabilities and a consistent look and feel across any device and from any location. "Those things really make a big difference across the enterprise," said Cunningham. "Whether they're in the office or at home, they're seeing the same thing when they log in."

But that frictionless experience cannot come at the expense of security. Citrix provides secure access solutions that take a zero-trust approach to security. Unlike a traditional on-premises virtual private network, Citrix solutions provide granular access to both software-as-a-service and internal Web apps, without needing to give them access to the full network, as often happens with a virtual private network-based solution.

"Security is about providing a balance between your employee's needs with the obstacles and risks that arise from enabling a truly adaptive workplace, and workshop," said Pentecost.

Final Takeaways: The Human Factor

Throughout the Briefing Center, the speakers frequently returned to a common theme: The importance of cultivating a cyber-savvy workforce. Here are three key points they made:



1. Don't limit education to formal training sessions.

Cybersecurity should be woven into daily conversations, Ngatuvai said.

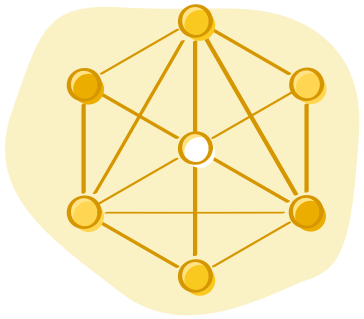
"It never hurts to always bring up security in discussions," he said. "Yes, there are the people who will tune you out automatically, because it's like 'Hey, I know, I know,' and that's OK. But the risk is, there may be a number of people that have taken the annual security awareness training that don't actually understand what phishing is, and what it would mean to them."

The more you bring it up in conversation, the more comfortable people will be saying, "Hey, you know what, I don't know what that means. Can you tell me a little bit more about it?" said Ngatuvai.

2. Don't let apathy set in.

Good cyber hygiene should be reinforced in multiple ways, said Cole. CBP, for example, runs exercises in which the agency phishes its own employees to see how many recognize a risky link. "If people do click, we make sure that they get the training that they need," Cole said.

CBP also provides a simple tool that people can use to report real-life suspicious links. And the agency is automating the collection of those reports to ensure that the security follows up on them — and then circles back to employees with updates.



3. Don't treat security as just another IT issue.

Cybersecurity should be seen as a shared responsibility across the workforce, said Citrix's Cunningham.

To support this work, Citrix tries to bridge the gap between an agency's HR and IT departments. "HR was always in one side of the building, IT in another," Cunningham said. "The only thing that brings them together is communication and cooperation."

Together, HR and IT can help cultivate what Citrix calls a "digital workforce" — one in which everyone sees cybersecurity as an integral part of the work they do and the mission they support, he said.

One way or another, our speakers said, any effort to improve cybersecurity always must address the tricky but vital human factor.

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