FEDERAL NEWS NETWORK

EXECUTIVE BRIEFING SERIES:

Balancing Cybersecurity and Collaboration

Sponsored by THUNDERCAT TECHNOLOGY

cisco Partner

THUNDERCAT TECHNOLOGY

CISCO Partner
Gold Certified

The Cisco Unified Communications Solutions delivers the right collaboration experience to any device, including voice, video, messaging, mobility, and web conferencing. Empower people to engage anywhere, using secure solutions.

---

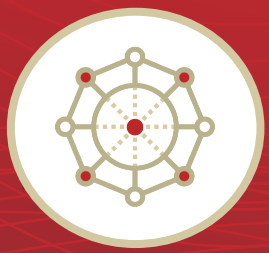
1 Unite applications and endpoints

2 Choose the right endpoints

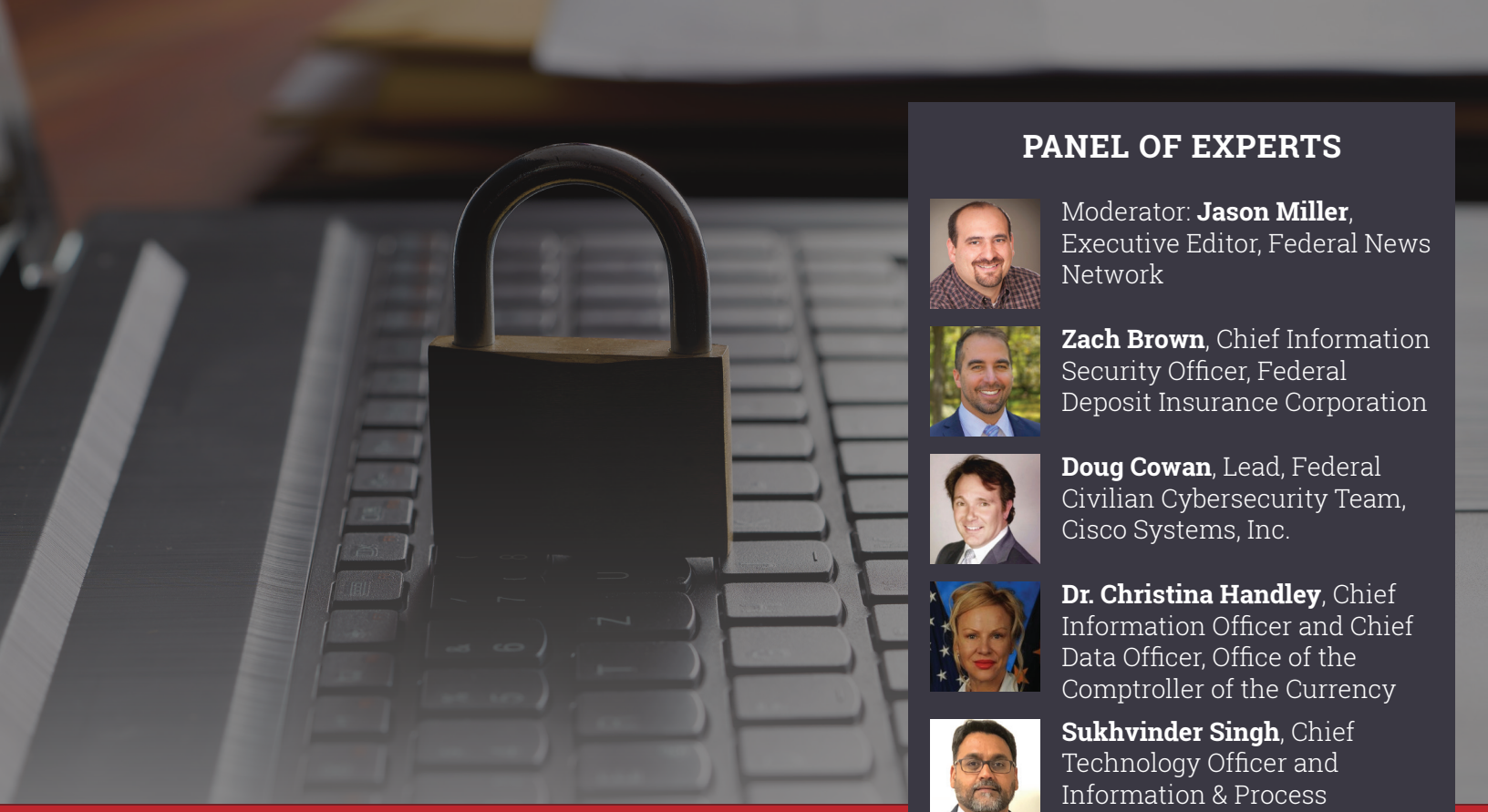
3 Secure conferencing anywhere

4 Move collaboration to the cloud with FedRAMP-authorized collaboration and video conferencing systems



THUNDERCATTECH.COM/PARTNERS/CISCO



Balancing security, usability is the future of remote collaboration

PANEL OF EXPERTS

Moderator: **Jason Miller**, Executive Editor, Federal News Network

Zach Brown, Chief Information Security Officer, Federal Deposit Insurance Corporation

Doug Cowan, Lead, Federal Civilian Cybersecurity Team, Cisco Systems, Inc.

Dr. Christina Handley, Chief Information Officer and Chief Data Officer, Office of the Comptroller of the Currency

Sukhvinder Singh, Chief Technology Officer and Information & Process Management Division Chief, United States Agency for International Development

Kurt Steege, Chief Technology Officer, ThunderCat Technology

Gary Stevens, Deputy Chief Information Security Officer, Executive Director for Information Security Policy and Strategy, Department of Veterans Affairs

BY JASON MILLER

For many agencies, their video teleconferencing system was like grandma's china—you knew it was there, but only broke it out on special occasions.

Then the coronavirus pandemic hit, and the VTC became the oxygen of the federal government—they couldn't accomplish much without it.

Doug Cowan, who leads the federal civilian cybersecurity team at Cisco Systems, called the first few months during the pandemic an "initial land rush for capacity, [where] everyone had to be sure that they could have a platform in place in which people could access the network could get to some of those key applications."

Nearly every agency has a story about increasing network capacity, bandwidth and adding more virtual private network (VPN) licenses and the like.

"What the Veterans Affairs Department did was, we established a series of scrums to bring everybody together to walk through what the requirements set was, and then go off into various working groups and report back to the to the largest scrum. In general, we doubled our VPN capacity, and quadrupled

our virtual servers to support Citrix and the Citrix access gateway," said Gary Stevens, deputy chief information security officer at VA during a roundtable discussion sponsored by ThunderCat Technology and Cisco Systems. "We increased our phone lines, so that we could allow for the more conferencing for the remote users. It was about a 200% increase from February to May that we realized."

Stevens said VA ensured there was consistency, cohesion and strong security, including two-factor authentication across all platforms.

VA's experience during those first months of the pandemic is not unusual.

Now to sustain and increase productivity

But now as employees settle into the "new normal" of work and video calls are a comfortable and expected way of working, many agencies are starting to look at what's next and how can they sustain, even increase, productivity through better tools and capabilities.

Cowan called the last few months a period of "normalization" across public and private sector organizations.

"What we've seen probably in the last quarter or so has been a real move toward optimization. How are we ensuring that we're getting a better user experience? Whether that's across the tools, the elasticity of accessing things, or making sure that we have the appropriate security in place to get the performance that we want?" he said. "What we've seen is that a lot of the agencies that have consistent policy and plans in place to address their users, regardless of where they are, probably had the easiest road. Some of the other agencies were struggling a little bit more with different use cases, asking what's my policy look like now versus what was it when everyone was in the office? It was a bit more of a shift. But for the most part, we saw most agencies were in really good shape to move ahead."

The way ahead for many agencies is further integration internally as employees return to the office, and externally with customers and citizens who are demanding a better digital experience.

"We're going to have to now plan in this aspect in everything we do. Not only the systems and the public facing systems and services, but even how we do business internally, how we're configuring conference rooms, how we're interacting with the public using this video component and this remote component because we are not able to sit across the table from someone as easily. We're sitting screen-to-screen now," said Zach Brown, the Federal Deposit Insurance Corporation's chief information security officer. "This is how we're going to do it, and it has forever changed how we're going to do business."

Balance between security, usability

Brown added the FDIC is taking a risk-based approach to any new services or approaches because the key is to find the right balance between security and usability.

"These have to be more deliberative processes, more deliberative discussions about what it is we're trying to achieve. Are all of these services available from these collaboration tools necessary? If they are

or if they're maybe not necessary, the old 'must have versus nice to have.' But if there's an element or a feature to these services or tools that will enhance the way we work or add some business value that maybe we hadn't considered in the past we need to have those discussions," he said. "They're not the old lock it down until you need it. Sometimes it is, let's open something up because there's a true business value or a return to how we're going to enhance these services. So I think it's a much more mature discussion that is evolving in the background. Hopefully it catches on, gets some momentum."

VA's Stevens said because of the pandemic the old way of looking at tools and making decisions didn't work anymore, and through other tools like those from the continuous diagnostics and mitigation (CDM) program, an agency could better mitigate the risks of trying out new tools.

Kurt Steege, the chief technology officer at ThunderCat Technology, said software development and DevSecOps efforts across the public and private sectors have seen a huge boost over the last six-to-nine months.

"By having an open architecture, the agency is able to plug in all the different pieces they need, and then having the transparency into what is being deployed to say, 'we've got to test here, we've got to make sure that these particular mandates are met,' whether it's HIPAA or whether it's protecting personal information, I think that's something that's interesting because we are making sure that all of the different groups are all working together to provide production worthy deployments," Steege said.

Sukhvinder Singh, chief technology officer and information and process management division chief for the U.S. Agency for International Development, said because nearly 100% of all applications are in the cloud and because so many of its employees work across the globe, the agency has made collaboration tools a necessary part of its mission for years.

Security, business areas coming together

Singh said the challenges for USAID with collaboration tools have been bandwidth and security related.

"I think the security folks and the technology people, the engineering people have come closer and are willing to work in a closer fashion to meet the business requirements because there is always that [concept of] this is in my control and it's really up to the implementation for how you see that," he said. "There are different ways you can address the requirement. I think that's something I see happening more now. The need to collaborate to meet the business requirements in this remote working situation."

Over at the Comptroller of the Currency at the Treasury Department, Dr. Christina Handley, the agency's CIO and chief data officer, said moving collaboration and other services to the cloud is an opportunity to make OCC more effective in meeting its business needs.

"We look at the sensitivity of the data to be exchanged, and the features of the tools that support our information exchange, and that factors into our decision or guidance on an appropriate use of the tools. We leverage the guidance put out by the National Security Agency and by the Homeland

Security Department on security baselines," Handley said. "When making decisions by any particular tool, we look at those baselines for whether it's low, medium or high security levels. Then it's really just about the features and the information exchange that inform those decisions. We have a really robust security program that thankfully we haven't had to compromise too much of our usability to meet our security needs."

She added as employees return to the office, she expects them to continue using the collaboration tools.

"Thankfully, these tools meet our security requirements without compromising usability," Handley said. "As new needs arose, which is the ability to communicate using external tools provided by OCC regulated institutions, we collaborated with the institutions to ensure a secure exchange of information. I expect that COVID-19 significantly increased the use of our tools, and because employees are now more efficient, more familiar and comfortable, I think that that higher level of usage will continue over the next couple of years."

Rise of zero trust

Singh added finding the right balance between usability and security is paramount for USAID too because so many employees are located outside the United States.

He said certain technical challenges came to the surface during the pandemic and now need to be addressed in the short term.

ThunderCat's Steege said one way to achieve the balance that Singh and Handley are talking about is through a zero trust framework.

He said agencies have to understand the people, the applications and the data so they can protect them individually and together.

"How are you dealing with not just the zero trust, which handles the authentication, talks about the VPN, talks about IoT and access but then what are you doing about data loss protection (DLP), how you're incorporating threat intelligence, whether it's internal or commercially available feeds and all of those things and how you build that into an overall architecture to make sure that that your secure access is there," he said. "Everybody's on that path. Maybe they're not, in many cases, calling it zero trust, but they're there already."

Cisco's Cowan added for many agencies it comes down to enabling the workforce and the citizens to access the data they need, when they need it.

"I think what we're seeing is people starting to adopt a software-defined determination. They are asking 'where do I have to change?' How do I respond to it?' They have to quickly do an inventory, an analysis, to understand how they enforce security requirements and then adjust on the fly as they need to. So they've got something that's scalable, flexible, and elastic," he said. "It's not all one vendor. It's lots of vendors that have to be able to work together to share information, through things like application programming interfaces (APIs), through coordination and through things like orchestration and automation tools, in order for their employees to be effective. So I think that's probably where we're going to see remote work go. People will be working from anywhere, accessing the appropriate tools that they need."