EXECUTIVE BRIEFING SERIES:
Securing the Remote Workforce
Detect and respond to threats your way

With complete visibility, analytics and automated response

Tap into your full potential as a threat hunter with RSA NetWitness® Platform. Our industry-leading evolved SIEM and threat defense platform gives you all the capabilities you need to detect virtually any threat anywhere: end-to-end visibility across your entire IT infrastructure, advanced behavioral analytics and automated response. Be the threat hunter you’re meant to be.

Go ahead. Be you.

RSA NETWITNESS® PLATFORM
Learn more at rsa.com/publicsector
As they pursue modernizing their infrastructures and applications, federal IT managers must also deal with a shift in the structure of the workforce – at least in the way it works. The pandemic-induced shift to large percentages of employees teleworking will ebb some, but only some. It will leave large portions of agencies’ workforces operating remotely. The network still enables the work and mission to take place, only the network itself has morphed to accommodate the unprecedented numbers of remote workers. This all requires some new thinking about how to architect and secure it.

This thinking must also extend to contractor workforces, who also are likely to teleworking in greater numbers instead of in the federal locations they serve.

Larger departments have seen a doubling or tripling of the numbers of people accessing applications and data remotely, mostly through virtual private networks (VPNs). In some cases IT staffs have pivoted to support upwards of 150,000 concurrent users. A recent National Institutes of Health town meeting was viewed by more than 40,000 people. One official recently quipped that whereas his agency had 12 centers of operation, it now has 60,000.

PANEL OF EXPERTS

Robert Carey, Vice President, General Manager, Global Public Sector Solutions, RSA

Karen Evans, Chief Information Officer, Department of Homeland Security

Brian Gattoni, Chief Technology Officer, Cybersecurity and Infrastructure Security
Altered threat landscape

The threat landscape has changed as a result of the telework shift. For one thing, “our adversaries know we’ve changed the way we’re doing work,” said Karen Evans, chief information officer at the Department of Homeland Security. “They’re working from their homes; their equipment is onto their networks on a VPN. When that happens you need to change the way you’re managing the risk.”

The user has always been an important link in the cybersecurity chain. Now the need for inculcating users in good cyber hygiene – including security measures on their home networks – is more important than ever. Whatever training in cyber best practices they’ve received in the office, employees must be encouraged to understand the need for at least as much vigilance working from home.

“I’m working from home. I’m an employee of DHS,” said Brian Gattoni, chief technology officer at the Cybersecurity and Infrastructure Security Agency. “My wife’s working from home. She’s an employee of the Department of Interior. My kids are schooling from home” as students in a local public school district. “That means I’m an IT troubleshooter and security professional for two departments and a local government to make sure everything’s safe.”

Make no mistake: Attack volumes are up, particularly highly sophisticated phishing schemes devised with the understanding that people are at home and might be more likely to test that link embedded in an email.

You can’t rule out old fashioned hacking. Users with government issued PCs and the VPN are nevertheless using home, carrier-provided WiFi.

Others are using personal devices with a variety of operating systems. They’re potential routes for unwanted intrusion into browser-accessed applications protected with traditional user names and passwords, or even to cloud access security brokers.

“There is a lot of responsibility back on the employee in order to be able to make this work,” Evans said.

But agencies aren’t otherwise helpless.

They can implement a fundamental, if not necessarily new, technology that has become a must: two-factor authentication. Even VPN access becomes more secure when the password gives way to a better, second authentication factor such as a one-time-use 6-digit token issued on a smart phone app.

A second fundamental, Gattoni said, is awareness of the location of data, given that ultimately, data is what most bad actors are trying to get. With government-issued equipment and VPN software, agency staff can encrypt data both in transit and at rest on the device. Therefore, data security becomes a simple matter of maintaining physical control of the device.

Needed: Greater awareness

Some organizations have decided that mobile devices – smart phones and tablets – may not process or hold data locally, but simply display it. Standard PCs or notebooks – again because of their VPN software – are often treated differently because of their on-board encryption capabilities.
With all of the device and access diversity out there, beyond the network perimeter, maintaining full visibility becomes a challenge to IT and security administrators.

Maintaining cybersecurity “requires a more centralized look at that broad spectrum of devices, and being able to manage and monitor that stuff,” said Robert Carey, vice president and general manager of Global Public Sector Solutions at RSA.

It requires a holistic view and management of applications, data, networks, cloud and on-premise locations — what Carey calls the “diverse ecosystem.” The diversity itself is not a problem as long the agency’s security operations center (SOC) has visibility into all of the assets and activities occurring through the networks.

Printing presents a telework-related security question that encapsulates many of the concerns relate to securing remote employees. Gattoni called printing a good use case for the ongoing risk management discussion. An agency’s continuous monitoring program needs to show who is accessing and downloading what data, and whether remote users are printing reports or documents on home printers. Such activity presents several potential avenues for data exfiltration.

But, Gattoni said, allowing personal printing – under a risk management framework – might be preferable to the workaround employees might otherwise make, namely emailing sensitive documents to their personal accounts as a way to gain printing ability.

Better still, he said, is deployment of collaboration tools to display documents on tablet devices in a way to let people read and mark them up, such that the need for printing is lessened in the first place.

Regardless, “The insider threat program has totally expanded because of this hybrid environment we have,” Evans said. “The tools are there. We have to think about what’s the risk we want to manage, and be able to monitor it so that [information] goes to the SOC and we know what’s going on.”

Some data, particularly classified or controlled unclassified information (CUI), should never reach home printers or other devices. Carey said preventing that requires role-based access controls and a close up view of where agency and personal networks cross.

“When we want to control data, have we gone in and fine-tuned access to data sets or applications at the level that we want?” Carey said. “We have to stare at the problem with finer lenses than we have in the past.”

Until now, Carey said, application access and printing have largely occurred with a federal facility on the Ethernet network with the printer just down the hall.

**SOC’s evolve with automation**

Wider monitoring of a larger number of networks and endpoints balloons the log data subject to analysis by the SOC. How do SOCs cope in the era of mass remote access?

Agencies need a strategy to have recurring threats and routine countermeasures occur without human intervention. Indeed, many agency SOCs have deployed technologies that basically replace the eyes-on-screens watching for anomalies in operations with automation, so only serious alerts are filtered out and channeled to analysts.
Software-defined networks also add to the mix. They widen the diversity of assets on the enterprise network, moving as they do among on-premise and cloud facilities. As they’re removed or newly spun up, the SOC will require an automated way to make sure the new instances have the security patches that might have been issued between instances.

The SOC “is a ripe technology opportunity space for automation,” Gattoni said. Analysts should be “crafting playbooks, turning their intuition into decision science we can automate and leverage technology. Like service orchestration, automated response capabilities – some of which are in the continuous diagnostics and mitigation (CDM) pipeline – to get the easy stuff off their plate so they can concentrate on the hard stuff.”

Evans said she sees the SOC evolving by taking advantage of machine learning, artificial intelligence and quantum networks.

“The network, how we manage and how we enable the security on the network is actually going to change the way we manage what our threat landscape is,” she said.

One piece of evidence of that change, Evans noted, is a DHS initiative to combine the network and security operations centers. It enables faster handoff from the operations people when they see something amiss, to the security people, all in pursuit of both operational continuity and cybersecurity.

Trusted Internet Connection (TIC) 3.0 will aid the SOCs, or combined NOCs and SOCs. Gattoni noted early guidance has already gone to agencies from CISA to agencies on how TIC 3.0 can help them in what he called “advanced telework,” navigating changing architectures that encompass commercial clouds, greater VPN use, and virtual desktop services, all in zero trust modes.

A word on security videoconferencing: People need to exercise caution about what a view into their homes can reveal that might have security implications.

“What’s in the background and what are we giving away about personally identifiable information? You are giving people information as to what does your house look like,” Evans cautioned. Book titles, pictures of family members or easily identifiable possessions could compromise security.

With advanced telework here to stay, it’s essential to think of the network this way, according to Carey: “Every user is really now part of the network infrastructure. Every user is a cyber defender.”

All of the SOC data, the deployment of new defenses, and use of facilities certified under the Federal Risk and Authorization Management Program (FedRAMP) “doesn’t relieve the organization from the responsibility to monitor it,” Evans added.

Ultimately, the remote access boom will accelerate both cybersecurity and the validity of the notion that a remote workforce can accomplish the mission.

“Things we’ve been talking about,” Evans said, “the importance of modernization, of moving to the cloud: All of that has meaning now because you are enabling your workforce through that secure model.”