FCW Cybersecurity Summit

Sponsored by PCM-G THE RIGHT TECHNOLOGY, DELIVERED

Innovate to Alleviate Cybersecurity Pain Points

Enterprise-level support is a crucial element to help other efforts move forward, according to a panel of security experts.

Defending against cyberthreats can seem like a necessary evil. No one can disagree with its need or the challenges associated with finding the right mix of solutions to provide the best protection. To ease the challenges of protecting legacy systems, pushing through a cybersecurity workforce shortage, and getting results more quickly, federal agencies are turning to innovations in technology and policy.

For example, the Defense Department's (DOD) Office of the Chief Information Officer is working to address one of DOD's main pain points—the department's sheer size, scope, and complexity. The DOD is making enterprise decisions to address decentralization and existing IT, says Mitchell Komaroff, DOD's principal adviser for cybersecurity strategy, planning, and oversight and adviser to the deputy CIO for cybersecurity, during a recent panel discussion on "Security Innovations Making a Difference."

The DOD rolled out the Windows 10 secure baseline across the department, for example, migrating IT tsystems running Microsoft Windows. "The challenge becomes, from the standpoint of the Office of the Secretary, being able to achieve the kind of integration … across the entire department," says Komaroff.

And they're not alone is dealing with enterprise-grade challenges. The Health and Human Services (HHS) Department is looking to work around a workforce shortage, says Chris Wahlschein, HHS chief information security officer and executive director of its Office of Information Security. "[There are] just not enough good cyber people to go around," says Wahlschein. HHS is partnering with industry and academia to develop a talent pool.

Automation is another way to ease the workforce problem, says Matt Connor, National Geospatial-Intelligence Agency's CISO, director of the Cybersecurity Office and occupation manager for the cybersecurity workforce. "Increasing automation can be a force multiplier for our capabilities, from our defense capabilities or even from our governance, risk, and compliance; increased automation scales in a way that a person in a seat doesn't."

The NGA is putting a premium on speed. "Speed is a growth area for us," says Connor. "Moving at the speed of mission is actually now part of our mission statement." For example, it used to take nine to 12 months for NGA to issue authority to operate certification for cloud services. It recently issued one in five days as part of its "ATO in a Day" initiative.

One area cybersecurity officials need to study harder is IT supply-chain security, says Lauren Burnell, CISO and engineering services manager at PCM-G. The emphasis is on the perimeter and e-mail. Agencies also need confidence in the integrity of the IT assets they're introducing to their environments. "At the end of the day, all an adversary has to do to get onto a government—even classified—network is be the lowest bidder," she says.

> "Increasing automation can be **a force multiplier** for our capabilities."
>
> **LAUREN BURNELL,**
> **CISO AND ENGINEERING SERVICES MANAGER AT PCM-G**

None of these efforts will be effective without enterprise-level support, the panelists agree, "I don't think you can do it effectively any other way," says Connor. "From a risk aggregation perspective, from a transitive trust perspective, from the risk assumed by one segment to 'shared by all,' if you're not looking at it from an enterprise perspective, you're destined to fail."

That means policy changes may be necessary. For example, HHS' CIO has worked with the operating and staff divisions' CIOs on a unified IT strategic plan tied to the performance objectives of each of the senior executives in those divisions. "There's an element, whether it's working on shared services or enterprise IT or cybersecurity, that each of those senior executives has to be held accountable for," says Wahlschein.

Komaroff suggests other shifts, such as planning for migrating technology in a way that supports security and is part of budgetary planning cycles. He also advocates bolstering the CIO roles. "Strengthen the role of the CIO in order to be able to ensure that there's enterprise management of IT across the infrastructure," he says.