CISOs Discuss New Approach to Tackling the Cyber War

Shared services provide cost savings, but are not always the answer.

Abigail Blue

Wed, 09/11/2019 - 13:16

Photo credit: your_photo/iStock

In the process of IT modernization, getting rid of tech debt could lead to an improved cybersecurity landscape that would help federal agencies better fulfill their mission needs.

At the Department of Justice, Chief Information Security Officer Nickolous Ward believes turning security teams into developers and embracing a new model for cybersecurity is the direction in which government needs to go to become more agile, rather than constantly updating and patching old systems that are not nearly as secure.

“We’ve got to be able to be fast. We’ve got to use code, security as code,” he said at the Billington CyberSecurity Summit last week. “My goal is to really make security an enabler rather than trying to catch up and tell everybody ‘no’ all the time. I want to make sure that we are helping them complete their missions.”

Another component “critical” to the Justice Department in “fighting the cyber war” is shared services. The agency is a leader in security operations and has offered its services to other federal agencies.

“We just think it’s really important to have good, strong capabilities that can be leveraged across any agency, and you shouldn’t be trying to hoard those things,” said Ward.

Shared services offer unique opportunities and are particularly beneficial in terms of cost savings, agreed U.S. Citizenship and Immigration Services CISO Shane Barney. However, he is hesitant to fully accept them out of concern they foster a compliance mindset.

“It makes an assumption that you can check a box, and now you’re secure. Security is a proactive game,” Barney said in reference to the shared framework by which the agency's security operations center is assessed. He also has banned the word ‘compliance’ in his division, choosing to focus on risk assessment and mitigation instead, he said.

The shared services model certainly has its place in IT modernization, but only to the extent that “it doesn’t get applied so far that it becomes the standard by which we define ourselves.” In the case of small agencies such as the Export-Import Bank of the United States, shared services remain an integral part of operations.

“We rely heavily on the shared services and the economies of scale to get the prices down for some of those tools that we wouldn’t be able to negotiate on our own with only 500 users,” said Export-Import Bank CISO Stacy Dawn. “We have the challenge of being able to afford the tools that you have, and we’re held to the same standards from the Department of Homeland Security as the larger agencies ... We have a lot less tools, but we have the same mission to protect data."

Having the right tools is not the only challenge in efforts to improve cybersecurity, as federal agencies are struggling to attract cyber professionals into their workforce. Professional development training is an appealing offer to many employees, but it can be worrisome to executives.

The bigger picture is what all agencies should support, Dawn said, adding that employers should not be afraid to train their employees due to fear that they might leave. If an employee gets promoted to another agency, she said, “that’s better for the government as a whole," and if they leave for industry, “it’s still better for our country."

View printer friendly version
Federal Cybersecurity
IT modernization
Federal Workforce
U.S. Citizenship and Immigration Services
DOJ
risk management
Department of Homeland Security
Standard