VA, USCIS Leaders Talk Cybersecurity Threats and Opportunities

Agency CISOs discuss the future of cybersecurity.

James Mersol

Mon, 05/13/2019 - 11:04

governmentCIO
Tech Futures in Government
in partnership with The Washington University

Photo Credit: Geoff Livingston

The role of security in federal governments is always changing, perhaps now more so than ever. Agencies are learning how to include security throughout the IT development process rather than having them review products at the end of the pipeline and considering what role security can play in privacy. At the same time, CISOs must develop strategies to ensure their offices remain fully staffed and ready to respond to ever evolving threats, according to CISOs from the Department of Veterans Affairs and U.S. Customs and Immigration Services

VA CISO Paul Cunningham said there is no standard day for a CISO, and the daily work involves rapid tactical response to threats and incidents.

“There’s a workflow you get into,” said Cunningham. “First thing in the morning…on your way out of the door, you want to check to see what’s on fire, and if you need to make some phone calls before you catch the ride in.” A CISO's wider role is ensuring that “security always has a seat at the table” when it comes to strategic decision-making, said USCIS CISO Shane Barney.

Cunningham stressed the importance of including security along the entire process.

“Cybersecurity has a history of [being seen as] almost an impediment,” he said. “It becomes almost a self-fulfilling prophecy. If we’re not included early, then we show that there’s a lot of problems in the rollout. If we’re included early, we can help avoid some of those barriers and [get to] market early or on time.”

Barney said that a culture change both in the office of information security and the overall organization is "critical" to ensuring that security assists in the agency’s broader IT mission. By bringing all those elements into the room, they begin to see all the decisions being made,” he said. “They understand the risks that are being discussed and how that interplays with the mission they’re trying to accomplish.” It has not always been easy to foster this collaboration, he added, but it has also enabled his team to explain how it manages risk and negotiate plans to develop secure systems.

Cunningham and Barney further discussed the integration of privacy and cybersecurity. Cunningham is thankful that privacy is under the purview of the Office of Information Security at the VA, which has allowed the VA to include privacy throughout the development process alongside security. At USCIS, privacy is not part of the CISO’s office, but it is still a focus for Barney, who said he would love to see the privacy office utilizing a risk-based mindset and embracing an ongoing authorization process for privacy controls, as the Office of Information Security has done for risk management and threat analysis.

Both CISOs also shared their views on the recent Executive Order on America’s Cybersecurity Workforce and what it will do to address the coming shortage of information security professionals. Cunningham said one benefit is that it fosters standardization of security practices across agencies.

“By going out and working at other agencies…you’re providing more of a cross-pollination of ideas, so we can build a more homogenous workforce that allows people to see… that [they’re] a valued asset in a bigger organization.” He expects that greater recognition of cybersecurity subject matter experts will encourage agencies across the government to better connect those professionals to their missions.

Barney agreed that rotating cybersecurity professionals between agencies would allow them to "expand their horizons," an incentive that the private sector offers to cybersecurity employees. However, he added that the government still needed to figure out how to retain employees in the long term, "whether that’s through better exposure within the federal space [to the overall cyber mission], [or] giving them greater opportunities on the salary and benefits side.”

Finally, the CISOs discussed innovation and how it could help them succeed in the future. For Cunningham, security needs to be agile in how it responds to threats.

“We need to understand that as tech’s changing, we need to speed up and be more sensitive and bring solutions where we can plug in pieces and parts of cybersecurity instead of one set of controls.," he said. "I hate to jump on ‘as a service’, but we need to start thinking of ourselves as a service.”

USCIS has migrated to the cloud, said Barney, but he is concerned that agencies might chase after shiny objects in the future rather than thinking about the underlying technology from a risk perspective.

“I totally get the shiny object syndrome,” he said, “but I also understand the risks associated with shiny objects. Once you move on to the next, that first shiny object falls to the wayside, becomes unsupported, and becomes a larger risk to the organization. Learning to better wrap our hands around that innovation is critical to the future.”

View printer friendly version
USCIS

veterans affairs
privacy
workforce
innovation
CXO Tech Forum Tech Futures 2019
Non-feature
Standard