VA CISO's 6 Takeaways from His First 6 Weeks

Cybersecurity and risk-management strengths and challenge areas are key observations for VA security chief.

Wed, 02/27/2019 - 00:36

Photo Credit: wingedwolf/iStock

The role of the Veterans Affairs Department's chief information security officer is crucial in overseeing the integrity of its patients' electronic health records and overall IT infrastructure. For an organization so big, the role also requires understanding of its cybersecurity framework.

Paul Cunningham stepped into the role of VA CISO and deputy assistant secretary for information security in January, and his first six weeks have proved to be quite the learning experience. He shared six things he's learned about the VA and its cybersecurity at the Feb. 12 Healthcare Information and Management Systems Society conference in Orlando, Florida.

The VA is Big

As the second largest cabinet-level agency, the VA has a budget of $180 billion depending on the year. "That just blew me away," Cunningham said, which speaks volumes for the size of the IT and cybersecurity portfolio and its importance to the nation.

The VA has the 'Best Team' of Cybersecurity Professionals

Cunningham said he was touring the VA's cybersecurity operations center and was "amazed" by not only the technology and level of efficiency, but also the diversity and commitment of the team. As the new CISO, it's good to know those resources are available.

The Complexity of the Federal Space and its Requirements

Requirements come from all over — Homeland Security Department, Office of Management and Budget, White House executive orders, and so on — and they tend to continue piling up. "For the CIO and CISO, we have to kind of drill through these requirements, understand what they mean, how they tie to our mission and develop these larger strategies," Cunningham said, and they will eventually cover VA's core portfolio elements.

Not All Cybersecurity Personnel Know of these Requirements

This is a challenge, Cunningham explained. And although they're very technically capable, "a lot of cybersecurity folks don't really know [Federal Information Security Modernization Act of 2014]," including people providing services to the federal government. Even 44 U.S. code 3554, or federal agency responsibilities, outlines what the department has to do in the cybersecurity program, he said.

"If I was a vendor, that's probably one of the first places I'd look to see what is their requirement, what is the foundational guidance documents, and then where do I align something like that," Cunningham said. From there, vendors can identify if they have the proper assessments and policies in place to match those of the agency in order to meet requirements.

Policies and procedures need to reflect those qualities so vendors understand what they are responsible for and can implement the proper security plans with awareness training and testing, incident response and resiliency to bounce back from a security event.

Cybersecurity Personnel Are Not Well Versed in Risk Management

It's not enough to just read and talk about National Institute of Standards and Technology security and privacy controls and risk management framework; they have to be revisited and understood. At the organizational and enterprise risk level, the VA secretary is responsible for the department's information and information system. "That's where the governance comes in," Cunningham said, "and what I can do to help scope where the department needs to move toward."

From there, the CISO has a role in ensuring the department can meet these requirements, minimize risk and put in additional controls. But it's important to understand where in the environment the risk is, rather than just monitoring the problem through the controls in place.

"Try to get cybersecurity folks . . . stop what they're doing and look at the larger risk mission approach," Cunningham said. This will also be a challenge, as cybersecurity personnel aren't typically trained this way. "As we move forward and secure our health records, we want to be sure that we're looking at a sound risk approach. We're probably going to have to look beyond just the traditional

controls," he added. This means compensating controls, identifying where risk decisions are going to be made and who will be making those risk decisions.

Cybersecurity Personnel Need to Know the Controls, and Advise and Foresee

Being well-versed in these controls is part of the job, as is informing leadership about the risk the department is facing and what exactly the impact of that risk is. Once risk assessments are done and brought to the risk owner, the information should include implications and what can be done to drive the risk down.

But overall, Cunningham finds the VA to be risk practitioners. "They want to take risks, they want to be partners, they're not waiting for this problem to be solved, they're leading the way," he said, particularly as the VA continues to be a partner in trying to move technology forward to improve health care.

View printer friendly version
risk
veterans affairs
IT modernization
NIST
HIMSS