COVID-19 Accelerated VA's Cyber Development

The demands of a sudden remote work shift have fostered an integrated approach to cybersecurity.

Adam Patterson
Tue, 10/20/2020 - 10:45

The demands of the COVID-19 pandemic, particularly the abrupt shift to a remote workforce, has fostered the development of cybersecurity best practices at the Department of Veterans Affairs.
Speaking at an AFCEA event last week, VA Chief Information Security Officer Paul Cunningham detailed how the challenges of the pandemic presented unforeseen opportunities to better refine how information and network security are managed across the agency. This has been a special priority for the agency in light of its considerable scope of responsibilities.

“Also for VA, we have a fourth mission,” he said. "While some agencies were trying to get into a snow day mechanism to see how long this is going to last, we were actually trying to figure out how to bring more people on [the network] quickly and how to streamline that."

VA had to adapt its IT capabilities in response to telework, a process that raised serious concurrent cybersecurity imperatives.

“We had a big chunk of our workforce now remote. And we’ve all worked through snow days, hurricanes, those sort of things, but we've never had a national snow day," Cunningham said. "We had to figure out ways to make sure our gateways were configured correctly and be able to handle those amount of people that we're going to remote in."

This focus on bolstering security during a time of network configuration served to put cybersecurity at the forefront of VA IT concerns — resulting in greater attentiveness to information security as an integral part of IT management as a whole.

“I actually think it's an opportunity more than a risk. I think for years, cybersecurity people had been drumming on about the importance of cybersecurity. I think this moved it up a notch,” he said.

Another positive development has been a growing attentiveness to best practices among individual VA employees, as well as a greater understanding of cybersecurity as an enabler of IT modernization rather than an impediment.

“I think it opened up people's eyes where they were looking at it more from what part do they play because all of us play a role in cybersecurity," Cunningham said. "I think we saw this as an opportunity where cybersecurity can step in and show that we're actually business enablers, and we can help with the mission."
Additionally, Cunningham recognized that COVID-19 served as an active and honest stress test of VA systems, with the learnings drawn from the prior six months likely to be built into IT security development even after the close of the pandemic — particularly a focus on the use of DevSecOps and Agile methodology as part of the development cycle.

“Our risk threshold changed because we had to in order to keep the mission going. But we still use those same risk management practices. And NIST is just as applicable today as it was pre-COVID. So we want to go back and look at why we do what we do and how we do it. We’ll definitely find some old thought that maybe doesn't need to be there anymore, and will get the chance to clean out the closet so to speak. As we come back hopefully a bit leaner and more agile,” he said.