How HHS OIG, DHA Handle Cybersecurity Challenges During a Pandemic

Senior federal officials urge colleagues to adopt a human-centric approach to security.

Kate Macri
Fri, 09/04/2020 - 13:08

If federal agencies want to strengthen their cybersecurity posture in a significant way, they should invest in cybersecurity best practices exercises and human education, according to cyber-focused officials at the Health and Human Services Office of the Inspector General and the Defense Health Agency.
“It's really, in my view, the human element that contributes to how secure that we are,” said LaMonte Yarborough, CISO at HHS OIG, during GovernmentCIO Media & Research's CyberScape event this week. “With that comes requisites such as user awareness of some of the indicators they should look out for. I think phishing exercises are key.”

Firewalls, software updates and continuous, real-time visibility of access points on your network are all great, but if your employees are making basic cyber mistakes — like opening a phishing email — then you’re still exposing yourself to criminal and nation-state cyber actors. Cybersecurity education is key.

“You will never be able to fully eradicate scenarios bad actors might exploit,” Yarborough said. “The better we are able to educate our constituency, I think the better we will all be for it.”

Tom Hines, director of engineering and technology transformation at DHA, said the agency's cyber response begins with employee education and “reminding the workforce of the training they'd already received and best standard best practices.”

“Because we're part of DOD, training around security principles is critical and done so repetitively throughout the course of the year,” he said at the event. “It is required for people to access the network. If they don't complete their required cybersecurity training, which qualifies most of our people for operating at the secret level, then they don't get to participate in activities on the network; their network access is removed.”

DHA faced greater vulnerability and cyber challenges at the beginning of the COVID-19 pandemic when the agency shifted to mass telework. Because DHA dramatically increased its bandwidth and VPN perimeter to accommodate remote workers, it created more cyberattack surfaces and opportunities for criminal and nation-state actors to take advantage of workers.
“There was a considerable increase in our adversary activity at the start of the pandemic,” Hines said. “It’s not really evident when you walk into something like this the strain it puts on your [IT] infrastructure. You’ve quadrupled your bandwidth requirements at your enterprise perimeter. We spent a lot of time figuring out how to really do that and do that without compromising security. Those presented some very unique challenges.”

Despite the security challenges, Hines said he thinks the shift to mass telework ultimately benefited the DHA.

“I’m very happy we went through with it at this point — It's taught us how to innovate at a rapid pace,” he said. “Because of the DOD security posture and overarching constraints on the overarching network, we had to take down and restrict most streaming services, which included office collaboration services, most office conferencing. All of those things we had to work through to continue to perform our mission, and we're still working on those things to make them better.”

HHS OIG addresses cybersecurity incidents due to human error with additional cyber education. More applications and technologies won’t necessarily fix the problem, Yarborough said, if human employees make preventable mistakes.

“Once someone has been identified as clicking a [malicious] link and going to a site and inputting info, as opposed to just alerting them of their mistake and hoping they'll be better next time, we impose some additional remedial training requirements on them to hopefully make them better aware of what to look for,” Yarborough said. “That human element in my view is going to be the most critical.”

If organizations don’t crack down on human errors, he added, it can be “disastrous” for the organization. HHS OIG is exploring punitive measures for repeat offenders.

Federal organizations dealing with cybersecurity issues also face the challenge of defining accountability in the cloud era, where private companies may have access to federal data.
“There's been some degree of concern with transferring that risk profile to a cloud services provider,” Yarborough said. “A lot of agencies have done that — transferring that risk is fine, that's done all the time — but somehow they've lost the idea of being accountable for that data. While the cloud services providers are responsible for it, you are still accountable for it. Spelling out the right language in contractual relationships ... it's been a little nebulous.”

Telework is here to stay, so as federal organizations confront IT infrastructure and cybersecurity challenges in a remote environment may need to adjust their IT strategies to be more human-centric and mindful of how real people do work at home.

“Our lesson learned here is our capacity to be flexible and agile,” Hines said. “It's the snow day that never ended, right? The truth is as we looked, we had more ability and capacity than we even knew. This is not limited to security, it's all IT operations. ... We now have better tools, and they're more widely deployed. I don't think we sacrificed security, I think we enhanced our posture overall.”