Cybersecurity's Critical Role During the Pandemic

The last thing federal agencies, especially health agencies, should do is allow their cyber vigilance to slip.

Kate Macri
Tue, 10/20/2020 - 08:28

When the COVID-19 pandemic hit, federal agencies knew they had to prioritize cybersecurity as employees shifted to telework. The Cybersecurity and Infrastructure Security Agency worked quickly to ensure federal agencies had the tools and guidance they needed to keep their data safe.

Since the pandemic highlighted different needs across organizations, agencies learned to pick and choose which cyber tools and approaches best fit their mission.
“Modern computing environments are a hybrid state at all times,” CISA Chief Technology Officer Brian Gattoni said during an AFCEA Tech Summit fireside chat last week. “It doesn't help us to talk about managing risk by just removing a capability unless it’s a stark threat, you have to manage yourself through the risk of evolution. VPNs may provide unique access and are also ways to protect yourself while you move to something a little more secure. There's no immediate advanced solution that's going to solve everybody's problems.”

The Food and Drug Administration addressed cybersecurity strategy right away because the agency knew the significant part it would in the pandemic response and knew it needed to be secure.

“We knew pretty early on that cybersecurity was going to be a significant concern going into this,” said FDA CTO Vid Desai during the fireside chat with Gattoni. “Not on just the teleworking side, but we were going to do some work that was going to play a critical role in dealing with the pandemic.”

The FDA elevated its cybersecurity posture, he said, “and we've remained there since then, letting people know this is the time where we really need to remain guarded. All the things you'd typically expect the nefarious folks to do started happening. It was good for us to be proactive in the stance we took.”

The Department of Health and Human Services beefed up its cyber operations at the beginning of the pandemic for the same reasons.

“We have to protect all the HHS data from [Centers of Disease Control and Prevention] to [the National Institutes of Health] and FDA,” said HHS CISO Janet Vogel in a subsequent panel on network security. “We also have to reach out and help others who may not be as cyber savvy or have problems in delivering health care.”

Vogel said her agency's cybersecurity push meant becoming more comfortable with a higher degree of risk.
“In cybersecurity, we rushed to the issue,” she said. “Guess who is accepting risk now? It's a cybersecurity community — it's us. Usually we're so risk averse, but some of the things we've had to do due to COVID, we're accepting risk and moving forward faster than ever.”

Some federal agencies, like U.S. Citizenship and Immigration Services, faced immediate funding challenges due to the nature of their operations. Because USCIS gleans much of its funding from interview and naturalization ceremony fees, the agency had to take a hard look at its operations and become tighter and leaner.

But instead of slashing cybersecurity budget and operations, USCIS CISO Shane Barney said the agency “didn’t touch” it.

“We still had to operate, the cybersecurity didn't go away,” he said at the event. “There were some new risks introduced that we have to handle. On the one hand, trying to grapple with the funding aspects and how to handle that, at the same time maintaining the operations of the agency. It became a really interesting balancing act.”

The pandemic prompted the FDA to explore new security measures, like zero trust.

“People are spread out in a very distributed manner and interacting with people and data in distributed locations,” FDA's Desai said. “The way we secure them is fundamentally changing. At the FDA, we've been doing a lot of thinking around zero trust principles. Those are the things that allow us to transform the legacy network to a new way to start thinking about the highly distributed world we live in.”

At HHS, data sharing with national security-minded agencies like the Department of Homeland Security and the Defense Department became a top priority.

“One of the big changes is silos where we would be focused only on intelligence or cyber or defense-type things. All that's broken down right now, we are all one team,” Vogel said. “That's making us much more successful. There's a generosity that we've seen that's been very heartening.”
Gattoni said federal agencies should hone in on cyber hygiene basics like patching, real-time monitoring, identity and asset management, and work with CISA to develop customized cybersecurity plans for specific agency needs. The last thing federal agencies — especially health agencies — should do is disregard cybersecurity despite the pandemic’s disruption.

“We have nation states out there right now trying to disrupt our success, and it's something we need to make sure we deny,” Gattoni said. “The stakes are high; success is mandatory here. We have to work hard to make all that data actionable in terms of insight and intelligence to our stakeholders.”