Nextgov

Cyber Officials Swear They Aren't the Enemy

Brandi Vincent
APRIL 23, 2019

https://www.nextgov.com/cybersecurity/2019/04/cyber-officials-swear-they-arent-enemy/156493/

Federal cyber officials want to help agencies build more secure health care systems, not just say no.

Cybersecurity and patient privacy must be baked into health care practices, systems and devices across the sector through early buy-in from medical and information technology professionals, federal officials said Tuesday.

Cyber officials told a health care forum hosted by ACT-IAC that the greatest challenge they're facing is people, not technology.

It's imperative that the IT professionals who are building use cases, systems and applications do not view the chief information security office as an entity that simply ensures they will meet certain standards and check off certain boxes, Tom Schankweiler, information security officer for the Center for Medicare and Medicaid Services, said.

"The right conversation is the one where they say 'how can we build [security and privacy into] the earliest thinking or concept of a design? How do we start to really build security into it and how do we put that patient and that privacy at the center?'" Schankweiler said. "And so it's not just about basic education. It's about that cultural change and getting people to really buy in."

CMS Chief Information Security Officer Janet Vogel agreed. She also noted it's necessary to help IT and cyber professionals come together to work on the same page.

"Everybody thinks they are doing the right thing, but if you think about IT, what are their goals? To be faster, better, cheaper," she said. "So with cyber, if we don't infuse this thinking from the very beginning of a project and make it second nature, we are going to

fail and our result and the sum of it is going to be less than the combination of all the parts, because we will not have succeeded in connecting them or making them effective."

IT professionals are frequently charged with designing architectures of the enterprise, growing out applications that are used, and making important decisions about how systems are implemented. However, Bruce McCulley, chief information security officer for the HHS Office of Inspector General said he's frequently found that development teams will try to fly under the radar and not involve cybersecurity teams in their work, out of fear that security professionals will make their jobs more difficult by telling them what not to do.

By the time cybersecurity auditors are involved, it's too late to ensure systems are secure.

"What we need to do is recognize that [IT professionals] are really trying to do the right thing. And we should try to promote good practices, enable mission goals and get everybody into a shared mindset rather than talking past each other," he said.

Like IT professionals, it's also necessary to guarantee that doctors, nurses, clinicians and other health care professionals also understand the significance of stewarding privacy and cybersecurity to best impact patients' experiences.

"If we don't bake in health care professionals into cybersecurity, how do we expect cybersecurity to be effective for the health care professionals? A doctor, or a nurse, or a clinician—why would they listen to me?" said Servio Medina, the Defense Department's chief of cybersecurity oversight, governance, and security. "We need to enlist [health care professionals] in order to make the messaging effective and meaningful. So, again, to the point: Everybody is involved in this."