Adoption of a commercial electronic health record will allow for fast adoption of emerging tech at the Defense Health Agency.

Mon, 03/04/2019 - 11:34

How are you approaching automation or other tools in cybersecurity efforts?
Automation and tools are important, but it's just really a piece of what we do overall. And really at the end of the day, it's the basic blocking and tackling that I think is the most important.

The way the spectrum works is you start off at the Department of Defense level with four or more D-Controls that are based on these standards. Then to that, we add security technical implementation guidelines, STIGs, that disestablishes — and you can think of those as basically best practices for configurations of individual product. Then to that, we add two-factor authentication for every single-privilege user account and for the vast majority of non-privileged user accounts.

Then, we have a standard methodology — actually, a pretty formal methodology — of how we implement patching of different severity and vulnerabilities. And to that we add our own tools, on top of the DISA tools, where we manage risk management framework — a system called eMass. On top of that, we then have our single new network that has a whole suite of security tools used by our CSSP and cyber operations center. So, at the end of the day we have all those formal methods, and then before we connect something on the network, [we have] the risk management framework implementation and evaluation [which] we take very seriously.

For some systems complex systems, it can take over a year to go through that process because there are hundreds and hundreds of controls. I have a workforce of about 225 people across the entire system that do nothing but risk management framework. Now over time, with a single network and standardization of medical devices and kind of moving back from that owning one of everything, I hope to reduce that number. But all of those things together — the tools, the people, the processes, the formal processes — really are what enable good cybersecurity, and I'm pretty comfortable with where we are.

**What emerging technologies do you see playing a key role in the future of IT at DHA?**
The adoption of a commercial EHR. One of the best things that's going to do for us is allow us to adopt new technologies as the commercial world adopts them as they get integrated into Cerner Millennium as a product, so we're going to get the best practices across the board for that. So that's one thing.

On the cybersecurity front, I'm really interested in some of the new AI technologies for micro-segmentation, especially in cloud environments — not necessarily the use cases that the vendors come to tell us about, but you know, in terms of say flattening the whole network. But I really like some of the things that we could use in the cloud to help separate us from other cloud tenants.

View printer friendly version
Federal Cybersecurity
Defense Health Agency
emerging tech
electronic health records
automation
Contains video
health
national security
Video