Despite Slashed Cyber Budget, HHS Fights Off Billions of Attacks Weekly

A treasure trove of health data makes the department a primary target.

Mon, 10/23/2017 - 09:09

The federal agency responsible for housing and protecting hundreds of millions of Americans' most sensitive health data spends less on cyber defenses than recommended but manages to successfully ward off a bombardment of cyberattacks every week, according to one of its top officials.

The Health and Human Services Department has all the health data of those using Medicare, Medicaid or health insurance through the Affordable Care Act, and at least one-third of Americans’ personally identifiable information, according to HHS Chief Information Officer Beth Killoran. This treasure trove of data makes HHS a primary target.
“If that doesn’t say that we need to make cybersecurity our No. 1 priority, I don’t know what it is,” Killoran said at GovernmentCIO Magazine’s CXO Tech Forum on Oct. 19. And because attackers today go after people's health history, rather than credit card and Social Security numbers, data protection is more important than ever.

Consider the Food and Drug Administration, an HHS component with over half a billion breach attempts a week — and that’s just one operating division.

“Imagine how many we have to fend off on a given week,” Killoran said. “And so if you look at that and you look at how much we’re spending on cyber, it’s just monumental what our staff is able to do.”

On average, departments are recommended to spend about 6 to 8 percent of its total IT budget on cyber, but HHS is spending about 3 or 4 percent, and continues to fight off sophisticated breach attempts without compromising data, Killoran said.

That’s in addition to making sure the department is doing what it has to do around Continuous Diagnostics and Mitigation and its EINSTEIN system, which detects and blocks cyberattacks from compromising federal agencies.

Though Killoran understands what HHS has to do from a federal perspective, it’s more than just thinking about — or reacting to — cybersecurity in terms of a mandate or audit. It’s about the need to adopt a strong risk management model and fully understand threats and risks, to be proactive rather than just reactive.

Killoran said it starts by identifying high-value assets, modernizing them and building in protection capabilities. Similar to industry’s concept of quality control or quality assurance, the ability to hack into a system is a vulnerability, and that vulnerability is a quality assurance problem; so it’s making sure those problems don’t exist.