DHS Seeks Partnerships to Counter Emerging Threats

Secretary Kirstjen Nielsen says the range of threats is too big for any one organization to fight alone.

James Mersol

Fri, 03/22/2019 - 12:50

alexsl/istock.com

Networked devices are becoming ubiquitous both inside and outside of the government. The Department of Homeland Security predicts these devices will soon be a critical part of every aspect of our daily lives, including not only communications, but also education, health care and other functions not traditionally associated with the cyber realm.

However, DHS cautions that as the “internet of things” grows rapidly, the number of risks grows just as rapidly, if not more so. The prospect of a hyperconnected world is spurring the DHS Science and Technology directorate and the Cybersecurity and Infrastructure Security Agency to rethink the way it approaches cybersecurity.

At the 2019 S&T Cybersecurity and Innovation Showcase, William Bryan, senior official performing the duties of the under secretary for Science and Technology for DHS, estimated that most attendees used “at least five” networked devices before the day’s events began — devices that might include cell phones, laptops, smart-home security systems and, in Bryan’s case, a Bluetooth-enabled coffee mug, which allows him to control the temperature of his coffee.

“I don’t know how I went 60 years without one,” Bryan joked.

Networked kitchen appliances are only the beginning. DHS Secretary Kirstjen Nielsen estimated there are 20 billion devices connected to the internet today. “By 2025, we expect that number to grow to 75 billion,” she predicted. “We will be living truly digital lives.”

It is this changing landscape and changing posture — “the future of cybersecurity” that keeps Secretary Nielsen up at night, she said. “It's not a matter of if we are attacked, or when, but it is how long we can withstand, and can we innovate while under attack?”

Because of the boom of internet of things, Nielsen said DHS is focused on how to manage risk. This approach hinges upon DHS partnering with other government agencies, as well as academia and the private sector, to present a united risk mitigation model. The range of threats will become so widespread that neither DHS nor any other agency can handle the job alone.

“We recognize that we can't expect any one organization to fight destructive malware, ransomware or rogue nations' cyberaggression. That's simply not a fair fight.” Nielsen said. “We want to partner. We're trying to find ways to leverage all of our capabilities and capacities across disciplines so that we can stay on top of the emerging threats.”

Such a broad range of threats requires a broad range of strategies and defenses.

Partnering for Solutions

Officials from CISA underscored the importance of working together to counter emerging threats.

“We don’t develop our own technology anymore,” said Martin Gross, director of the Office of Cybersecurity and Communications at CISA. “We rely solely on what’s available on the commercial marketplace, so we need to figure out how to bring that in a lot more quickly.”

Focusing on the effects of partnership in day-to-day operations, Gross saw the greatest opportunity for improvement in data analysis tools and security on the back end of emerging technologies.

Gross also went further than discussing public-private partnerships, suggesting that risk awareness is a civic value.

“There’s a broader societal problem about the willingness of people to push technology forward … before we understand how that technology is used and what the security implications are,” he said. “We need to start thinking about that from a risk perspective.”

CISA director Christopher Krebs was optimistic about the future of partnerships between DHS and the research and development community. He looked forward to discussing three specific topics at the 2020 DHS S&T Cybersecurity and Innovation Showcase: an infrastructure to analyze threats at an unprecedented scale, data analytics technologies to counter threats proactively and systems to protect mobile devices at the data level.

“The research and development community is going to help us get ahead of the next threat,” Krebs said.

View printer friendly version

Federal Cybersecurity
Department of Homeland Security
partnerships
emerging tech
Standard