Homeland Security is Building Collective Defense Against Adversaries

Cross-sector bidirectional information sharing will help DHS address critical infrastructure risk.

Amanda Ziadeh

Fri, 07/20/2018 - 15:57

Left to right: Dylan Conner, CTO, ID Technologies; Scott Bean, assistant director for IT Infrastructure Division, FBI; Sabra Horne, director of SECIR, DHS; Jacob Torrey, program manager, DARPA. Photo: GovernmentCIO Media

The Homeland Security Department's Stakeholder Engagement and Cyber Infrastructure Resilience division is collaborating with its private and public sector partners to create a "collective defense" against cyber- and nation-state actors.

"We're working across all 16 infrastructure sectors to ensure that we're sharing that which we know in the government, as well as hearing from private sector and

[state, local, tribal and territorial] partners to gather the information that they know," Sabra Horne, director of DHS' SECIR, said at the July 17 GovernmentCIO Media CXO Tech Forum on national security in Arlington, Virginia.

"So together, we're stronger," she added.

Reducing Systemic Risk

Within the 16 critical infrastructure sectors, which includes an election infrastructure sub-sector, is the particular importance on the electrical sector (under the energy sector), financial services sector and IT sector.

"We feel that those are very important in terms of us understanding how they're interconnected," Horne said.

That's because of the systemic risk associated with these sectors. Horne said it's "virtually impossible" for these sectors not to be connected to another sector, and she cited the WannaCry ransomware attack as an example.

"Within almost 24 hours, over 150 countries were somehow impacted by a relatively simple ransomware cyberthreat," she said. "Yet, because of the interconnected nature of how our infrastructures work, there were very many who had been affected by the unfortunate incident."

If one component of a sector is impacted, it's highly likely not only will other components be affected, but as will other sectors. So, addressing this systemic risk with government and private sector partners is crucial.

"We're trying to build what we call the 'collective defense' of what we're able to accomplish together," Horne said. "Which is together, we're going to be able to be stronger, and only by working together and knowing what each other knows we'll be better off."

SECIR is trying to understand that interconnectedness, the risks within each sector and how to collectively raise the level of preparedness. But trying to identify and assess systematic risk is an obstacle in itself.

Scaling and Prioritizing

“One of our biggest challenges is scaling to the challenge,” Horne said. “We see that there are cyberthreats that cross all 16 sectors . . . we’re trying to figure out, as quickly as possible, how we go prioritizing those risks so that we can utilize government resources to be most effective in addressing those risks.”

This prioritization falls back on the Section 9 critical infrastructure entities described in the Obama administration’s Executive Order 13636: Improving Critical Infrastructure Cybersecurity. That section articulates there are a finite number of very high-risk companies that, should they be impacted by a cyberthreat, would have the most devastating and cascading consequences across multiple sectors, Horne said.

So, SECIR makes sure it provides those companies with the information and resources they need to thwart cyberthreats, while also providing to those smaller and medium-sized business that lack the means to pay for, say, expensive private sector threat assessments. SECIR has been able to create roadmaps for those smaller businesses to help them identify which DHS resources would be most beneficial to addressing their needs.

Better Together

The private sector plays a key role in identifying the threats to critical infrastructure, which is why bidirectional information sharing is so important to SECIR.

The private sector, as owners and operators of more than 90 percent of the critical infrastructure, provides DHS with great insight into understanding who is being impacted by a cyberthreat, Horne said.

“There’s a responsibility that we all have in ensuring that we’re working together to raise that level of protection collectively,” she added.

And while these Section 9 companies rise above because they hold higher risk, Horne said it’s important to look across all 16 critical infrastructure sectors to identify where the cyberrisks are, and work with actual companies to define which risks exist.

As part of these efforts, Horne said DHS stood up a Tri-Sector Council with the

electrical, financial services and IT sectors. It focuses on identifying those areas of risk and works with DHS to develop incident response. The council is also looking for those triggers of cyberattacks across the three sectors so they can be addressed proactively.

And if there was an attempt to hit the U.S. with a digital critical infrastructure attack, Horne said she's looking to each of the critical infrastructure sectors to build their resilience, for companies to work together within their sector and with the government to take a deeper look at operational cyberincidents and adversarial attempts.

View printer friendly version
DHS
CXO Tech Forum: National Security
cyberattacks
cybersecurity
risk