Defending the Homeland’s Most At-Risk Critical Infrastructures

It’s a job too big, and far too broad, for just one government entity.
Sat, 07/07/2018 - 10:27

Securing the nation’s critical infrastructures, all 16 of them, involves cross-sector collaboration between state, local and federal government, and industry partners. That’s why bidirectional information sharing is crucial to Homeland Security Department’s Stakeholder Engagement and Cyber Infrastructure Resilience division

Sabra Horne, director of SECIR, says her division is working to understand the interconnectedness of the critical infrastructures most at risk — the electric, financial services and IT sectors.

“We understand that there is systemic risk, that when you have one sector, it’s virtually impossible for them not to be connected to another sector,” Horne says.

And the three sectors listed above have cascading and devastating consequences if they were to be hit with a cyberattack.

So, it’s important for the owners of these infrastructures, as well as other stakeholders involved, to work together.

“We’re working to help us all raise our level of preparedness together,” Horne says.

On the other hand, the Defense Advanced Research Projects Agency is looking at securing critical infrastructure from both the IT and operational perspectives.

“When you’re talking about critical infrastructure, the idea of fail-safe kind of means something separate from something in an IT infrastructure,” explains Jacob Torrey, program manager at DARPA. In an IT environment, it may mean defaulting to closing a port or locking someone out. But in an operational environment, if an oil well is on fire, for example, Torrey says fail-safe may mean defaulting back to allowing people in remotely to be able to turn that off and make something safe again.

With critical infrastructure, the IT world is being connected to the operational technology world, and Torrey is working on two projects addressing this crossover. One looks at how to protect legacy systems, which includes everything on market today, because once it has made its way to the shelves, “it’s already considered legacy,” Torrey says. He’s working to mitigate those vulnerabilities and provide broad, long-term protection. The other program focuses on configuring those protected system.

Watch the full panel above to hear more from Horne and Torrey, along with Scott Bean, assistant director for the FBI’s IT Infrastructure Division, and Dylan Connor, chief technology officer of ID Technologies.

View printer friendly version
Contains video
CXO Tech Forum: National Security
Sabra Horne
DARPA
Jacob Torrey
national security
Video