Meritalk: Counterintel Chief: Wrap HR into Security to Fight Insider Threats

NEWS
EMERGING TECH
CYBERSECURITY

Aug 7, 2018 | 3:49 pm

Bill Evanina, director of the National Counterintelligence and Security Center (NCSC) in the Office of the Director of National Intelligence, said today that the billions of dollars the U.S. government and private sector spend each year on cybersecurity are not being properly and efficiently utilized unless government and industry wrap human resources departments tightly into security discussions.

Evanina, speaking at an event hosted by Nextgov and Equifax, argued that HR represents an essential element in combating insider threats–which he called the biggest concern in nation-state espionage and theft of government and private sector proprietary data.

“We spend billions of dollars a year as a country on cybersecurity, bringing in CISOs and CSOs and CIOs, hardening up the information structure. We spend a lot of time hiring outside consultants, bringing companies in to facilitate, shore up our walls from a cyber perspective. Where is human resources in all this?” he asked. “Who are we bringing in inside our walls?

Evanina called for a new structure that incorporates HR into a holistic security process. “If you are the CEO of a company, or you’re on the C-suite, have you integrated your human resources folks as part of your enterprise-wide security process? If you haven’t, it’s a big mistake.”

He said that in the Federal government alone, the Federal Bureau of Investigation and Justice Department have indicted or arrested 15 people in the past 15 months for serious insider threat violations including alleged spies and unauthorized leakers. And he emphasized those were just the known, publicly-disclosed cases, and that the problem extends much further into the private sector.

“I would say it’s just as big of a problem, because we are losing our trade secrets and proprietary data at record pace right now,” Evanina said.

He referenced NCSC’s July 26 public release of its 2018 Foreign Economic Espionage in Cyberspace Report, which describes foreign intelligence efforts to mine U.S. intellectual property through cyberspace.

Evanina said he was asked by a reporter–at a press conference following the report’s release–if the proliferation of espionage via electronic means was the greatest threat. He responded, “No. The insider threat is still No. 1. This is just another vector or venue for how our nation-state threat actors steal our secrets. And not just our government secrets, but just as important, our proprietary data and trade secrets.”

To that point, he called out an FBI arrest of a General Electric employee last week, who is accused of stealing proprietary data on turbine and power plant technology. Xiaoqing Zheng is a U.S. citizen with ties to Chinese companies, and according to an affidavit, a search of his home yielded a document that explains resources the Chinese government provides to individuals in exchange for certain technology information.

Evanina said Zheng may have been stealing secrets for as many as ten years, and that Zheng’s ten recent trips to China should have sounded alarm bells. These

concerns prompted Evanina's call for a new way organizations should approach security.

"You have to be willing and committed to have a top-down, bottom-up mindset: 'How are we as a collective organization, whether in the government or private sector, going to, as a group, prevent and deter the theft of proprietary data and trade secrets?'" he said.

Evanina said this process "includes and starts with" with HR–and training the human resources department within every organization "to understand the threats that are out there" but which manifest inside the organization itself.