Private Sector Cooperation Essential for National Cyber Defense

The National Counterintelligence and Security Center emphasized the need for executive-level cyber education.

Adam Patterson

Wed, 02/12/2020 - 07:37

iStock/alexsl

The U.S. private sector is a crucial contributor for proactive efforts in national cyber efforts, according to Director of the ODNI National Counterintelligence and Security Center Bill Evanina.

“When you hear the word ‘counterintelligence,’” most Americans “think about a spy, the FBI, CIA, dark alleys in Vienna,” Evanina said at the Feb. 4 ICIT Briefing. I n contrast to the pre-internet paradigm of human intelligence collection that dominated the Cold War, Evanina detailed that data collection and remote surveillance are now primary means through which adversaries extract sensitive information about the U.S.

This is a particularly thorny issue, Evanina admitted, considering how much of America’s critical defense and security infrastructure is managed by a private contractor base.

“We need to expand not only accountability, but the authorities and awareness of who’s responsible for protecting our intelligence,” Evanina said.

The increasing digitization of data, trade secrets and sensitive information has been further complicated under a current paradigm of widespread data sharing between private conglomerates.

“Health care, banking, financial services — they own our data," he added. "They employ another company to store that data in the cloud. That cloud is then breached by a nation-state threat actor. Your data is now breached — are you blaming your bank or the cloud service provider?”

Despite the modern nature of this intelligence quandary, Evanina said that the best defenses against foreign collection are often relatively simple and rest on the age-old practice of basic trust verification.

“Does the People’s Republic of China use sophisticated intelligence tools to break into your company’s critical infrastructure and steal your [personally identifiable information]? No. They’ve always gotten it one way," Evanina said. "95% of all breaches that have occurred in the past 10 years have come from successful spear phishing attacks."

Responsibility for preventing this variety of data breach starts at the top. “Recent studies show that 78% of industry CISOs have admitted to clicking a link they haven’t validated,” he added.

Evanina detailed that the Defense Department and U.S. intelligence community are beginning to take a proactive approach in fostering cybersecurity best practices among their private-sector clients.

“You have seen some movement in the Defense Department with the deliberate compromise concept and with adding security as part of the procurement process. And I think when the DOD starts to mandate security with procurement for the defense industrial base, that will trickle down to suppliers,” Evanina said. “We see the threat, we see the penetration of third-party vendors by foreign nation-states. We just don’t do a good job of communicating that. The DOD will start the trend on that.”

The solution, Evanina continued, lies in taking a holistic approach to counterintelligence and cybersecurity.

“As the new [counterintelligence] strategy gets rolled out, we’re going to take a whole-nation and whole-society approach,” Evanina said.

This will require a twofold approach: greater intelligence community outreach to the private sector combined with adoption of information security best practices across the upper echelons of industry. The first of these will need to take into account the sheer breadth of vital capacities maintained by private enterprise.

“The government doesn’t make anything, we just buy from industry," Evanina said. "We have to do a better job of protecting industry.”

The second of these will require buy-in from company management combined with a human resources and background review process designed to guard against insider threats.

“The security of your company can no longer rest at the feet of the CISO and CIO. It now has to include the CEO, the chief data officer, the chief privacy officer, the general counsel and the head of human resources … we need to know who we’re hiring, and make sure the head of human resources know they’re a critical part of the process,” Evanina said.

This approach will require consolidation of the hiring and the clearance investigation process, a reform that is currently underway.

“What we’ve done historically since the 1940s is that we’ve had a human resources process and a security clearance process. We are merging those together now,” Evanina concluded.

View printer friendly version
Intelligence Community
national security
security clearance backlog
Defense Department
FBI
Standard