CISA Director Calls on His Cybersecurity Evangelists

'What More Can You Do?' is Christopher Krebs's Motto Going into 2020.

James Mersol
Thu, 09/19/2019 - 16:53

CISA Director Christopher Krebs speaks at at the DHS Cybersecurity Summit on Sept. 18, 2019. (Photo: Department of Homeland Security)

Cybersecurity and Infrastructure Security Agency (CISA) Director Christopher Krebs did something unusual at this year’s Cybersecurity Summit,. Rather than target his speech towards those in the audience, he instead mentioned he was preaching to the choir, and encouraged them to act as cybersecurity evangelists.
CISA wants to focus its efforts on reaching out to the agencies and firms that “aren’t in this room”, Krebs said. The mantra everyone should follow is “own it, secure it, protect it,” he said. “We need you to push this message out more broadly.”

Compared to the first Cybersecurity Summit, which invited only around 400 people to a small conference in New York City, CISA intentionally brought this year’s conference to Washington, DC and included thousands of people. The goal was to “take our collective experience and make it more accessible,” Krebs said, promising that next year’s conference would be even larger and more accessible, inclusive and diverse.

The crux of Krebs’ keynote address to the audience was “a play in three acts,” with not only the federal government, but also state and local governments, private sector and individuals serving as the protagonists. While act one covered CISA’s early days, and act two concerned current efforts, the most important part for Krebs was act three.

“What more we can do?” Krebs asked, advocating for a new, proactive perspective on cybersecurity. He later repeated those exact words, saying that would be his first question to Robert O’Brien, Trump’s pick for National Security Adviser. He also turned it around on the audience, asking, "What more can you do?"

The core of that perspective is a focus on engagement and education to build confidence and resiliency in the United States’ networks. The first step is moving away from fearmongering.

“Stop selling fear,” Krebs urged. “Fear sells, but we have far too much to offer.” He said sharing information about the problem is no longer enough to solve the problem. Going forward, each federal agency and private sector partner ought to think about their comparative advantage and what they can do to defend their networks against data breaches, ransomware and other attacks. Most government agencies are well aware of the problem and poised to respond it - collaboration will fast-track solutions.
After 23 counties in Texas and seven parishes in Louisiana suffered ransomware attacks to their systems, nobody is “shrugging [the threat] off,” Krebs emphasized in a press conference the next day. Instead, it is incentivizing CISA and its partners to augment its approach to threats and “put resilience into the system.”

These attacks also underscore the need for greater outreach and support to smaller agencies and local governments, Krebs said. He encouraged both public and private sector leaders to pursue local community outreach to better identify solutions to the problem, whether it is election security or attacks on the integrity of federal systems.

The epilogue of CISA’s “play” is “unwritten,” Krebs said, “but I want to fast forward to November of next year. What are you going to do to protect 2020? What is your company or organization going to do? Are you going to understand the requirements when you go to vote, if there’s a bad day or the power goes out?” CISA and its partners want to ensure every American plays a part in answering those questions and are confident in their answers.

View printer friendly version
Federal Cybersecurity
election security
Christopher Krebs
cyberattacks
Standard