CISA Director: ‘Cybersecurity Has a Posse'  
Coordination with partners at all levels continues to be a focus for the agency.  
James Mersol  
Wed, 02/26/2020 - 16:37

Photo courtesy of the the Cybersecurity and Infrastructure Security Agency

One of the Cybersecurity and Infrastructure Security Agency’s (CISA) priorities as the nation’s risk advisor has been to build relationships as it works to “defend today, secure tomorrow,” as the agency’s motto goes. At the 2020 RSA Conference, Director Chris Krebs explained that the agency has an additional motto — “cybersecurity has a posse” — underscoring the role everyone plays in building resiliency and defending the nation from cyber threats.
First, Krebs urged private sector to come to CISA whenever it experiences a ransomware attack or data breach. He understood that some companies are concerned that disclosing an attack might expose them further, but reminded the audience that it does not name victims.

“We send [threat information] out in an anonymized way,” Krebs explained. “What we’re trying to do here is understand the landscape — understand the conditions on top of it, and what the adversary might be doing — and get that out so the next victim might not happen. This is particularly important in the broader ransomware conversation.”

Krebs urged organizations faced with ransomware to contact CISA rather than consider paying the ransom. Even if paying the ransom seems like the quick and inexpensive option, in CISA’s experience, ransomware keys only work 20 to 50% of the time and “you’re validating the business model.” CISA is working with small and medium-size organizations to build a proactive defense against ransomware and organizational resiliency to lessen the likelihood of and damage from an attack.

Krebs also explained that he believes the benefits of information sharing far outweighs the risks of disclosing to adversaries what the agency knows.

“I’m not a big fan of security by obscurity,” he said. “I don’t think it works. I think that we need to get ahead of the curve in a collective defense approach where ... if everybody does work together and everybody pulls together as a team and shares information rapidly enough, we can build better defenses.”

One success story for collective defense has been the response to the threat of Iranian cyberattacks. CISA was already in an enhanced posture ahead of the American strike on Qassem Souleimani, Krebs said, and enacted a plan to reach out to around 26,000 individuals to inform them about Iranian tactics, techniques and procedures.
Krebs underscored that election security is a continued priority for CISA, and the agency is working closely with the 8,800 election jurisdictions to implement risk assessments and security procedures. Previously, the agency was “pushing for paper backups,” as Krebs outlined during a later press conference, and is still working with the 10 to 20% of jurisdictions that have yet to implement them. Now, Krebs said, CISA has an additional focus centered on protecting voter registration databases.

“We tried to figure out where the risk really is across these systems,” Krebs said, “and what we discovered, not surprisingly, is the areas where information is centralized, and it’s highly networked — that’s where the risk is. And where is that? Voter registration databases.”

“100% security is not achievable,” Krebs said — a message echoed by many in both the public sector and private sector across RSA. CISA has been hard at work with its partners over the past year on increasing resiliency in these systems. Even if a nation-state actor or even an opportunistic criminal tries to launch a ransomware attack on a voter registration database a week before the election, the goal is to minimize the damage to that system and not derail the election.

“Again, it’s like any other ransomware event,” Krebs said. “You have an offline backup that you test, and you practice and you have a plan.” Paper backups at the state and precinct level are an important component of this resiliency.

Above all, Krebs emphasized that despite these risks, the American public should be confident in the integrity of its elections.

“2016 was a front-to-back wake-up call across the federal government,” Krebs said. “There is no single issue that I’m involved in where I’ve seen this level of engagement, clarity of purpose and jointness of mission. The Intelligence Community, federal law enforcement, my team and the election assistance commission — everybody is at this issue as hard as any other issue that I’ve seen.”

Krebs concluded by encouraging everyone to get involved in collective defense, including through sharing knowledge and best practices, disclosing threat information or even applying to work at CISA.

“We are only going to be able to do this together,” Krebs said.