Agency CISOs Plan for New Programs, Partnerships, Personnel in 2019

This year's efforts include new monitoring tools and recruitment strategies.

James Mersol

Mon, 04/01/2019 - 12:38

Urupong/iStock

As the federal government approaches the end of the first quarter of 2019, many federal agencies are looking at what they accomplished in that quarter, despite the partial government shutdown, and looking toward how to plan and implement new cybersecurity measures for the rest of the year and beyond. At the 2019 RSA Federal Summit, chief information security officers from government security agencies both large and small shared their outlook for security in the year ahead.

The CISOs highlighted deficiencies in their authorization and risk detection systems, but looked forward to advances in those systems in 2019.

“We are in the process of implementing a version of the [RSA] Archer tool so that we can see workflow and one source for the [authorization] documents and be able to close vulnerabilities through an automated scan,” said Cris Brown, CISO for the Nuclear Regulatory Commission. Brown added that the system is a major upgrade from the current system, where all authorization requests are submitted via email. “I feel like I’m continually in an email jail because I can’t find what it is that I need to look at to authorize and send to the CIO,” she said.

Stacy Dawn, CISO for the Export-Import Bank, said that EXIM was looking at similar tools for continuous diagnostics and management (CDM). “What we want to do is make sure we have our on-prem and cloud [data] going into the same tool,” Dawn said. “Right now, we’re reviewing logs, but if you’re reviewing logs for on-prem and for Office 365, you can’t see anomalies.”

New CDM tools will allow CISOs to compare access logs for cloud systems and on-prem (on-premises) systems simultaneously and automatically flag anomalous behavior, such as the same account logging in from two different locations.

The agencies are stepping up their partnerships with the private sector, recognizing that while the private sector can offer new technologies to agencies, the agencies can also take the lead in sharing information about new threats.

Department of Health and Human Services CISO Janet Vogel highlighted HHS’ information sharing program, HC3. “We monitor and identify anomalous behaviors across networks,” Vogel explained. “We find out what’s going on, and we’re able to reach out specifically to areas and help them solve their problems. We also take all of that information and put it together in a way that is very understandable.”

Vogel said that the HC3 program published 85 reports to the health care and public health sectors last year that identified threats and explained how to protect against them. She hopes that more healthcare organizations will join HC3, especially medium-sized companies that are at risk of being hit with ransomware or other attacks.

“Anybody who wants more information, we’ll give it to you,” said Vogel. “When we find something like SamSam, we’re able to get the information out and have [our partners] block any of those attacks. We’re really active in that area, and we’d love to share more information.”

Agency CISOs are concerned in both the short and long terms about the anticipated 1.8 million-employee gap in the cybersecurity workforce. While cybersecurity and STEM programs at high schools and colleges or retraining programs like the Federal Cyber Reskilling Academy will help close that gap in the long run, the CISOs hoped to advertise the benefits of working for the federal government’s cybersecurity teams in the short run.

“[HHS] is not what anyone thinks of first when they think about cybersecurity,” Vogel said. “But we protect the health information for one out of three Americans, and we’re looked to [as the ones who] protect that data. So we use that information to reach out to people. Someone said earlier the mission draws people, and that is absolutely true.”

Dawn admitted that smaller agencies lacked the capability or budget to train new cybersecurity professionals like the large agencies, but added that they excel in expediting the recruitment process. “Our [human resources] is a lot faster at hiring, so when we have a position hit the streets, we don’t have the competition of tens or hundreds of positions opening up,” she said, “We can grab one or two employees before [the larger agencies] have a chance to do the paperwork.”

Smaller agencies can also provide a career where those employees can use a range of talents rather than focus on just one facet of information security.

“In a small agency, you just don’t have the personnel” to assign each of them to a single operation or project, Dawn said. “What’s nice is that our workforce gets to play with everything that they need, so it gives a lot more flexibility.”

View printer friendly version

Federal Cybersecurity
Health Human Services
RSA
Standard