CISA Looks at Partnerships, Data Protection Among 2020 Priorities

The new assistant director brings artificial intelligence background to the agency.

James Mersol

Wed, 01/15/2020 - 09:04

Photo Credit: Gwengoat/iStock

As “the nation’s risk advisor,” the Cybersecurity and Infrastructure Security Agency moves into its second full year with an eye on securing election systems before November, alongside its mission areas of protecting critical infrastructure, coordinating emergency response and defending the dot-gov domain from adversaries. 2020 also brings a new leader to the cybersecurity directorate: Assistant Director for Cybersecurity Bryan Ware.

In his first public appearance in his new role, Ware discussed the state of security and data policy for the Department of Homeland Security and outlined the priorities and key focus areas for CISA in 2020 and beyond.

Ware discussed CISA's role in building interagency public-private partnerships in security, rather than mitigating risk through regulation.

"We don't compel information sharing or vulnerability disclosures," he said. "Those are activities that we encourage and we enable — really, to do that, it requires partnerships."

Coming from the private sector before his previous role as the assistant secretary for cyber, infrastructure and resilience policy, Ware said that creating mutually beneficial partnerships is a goal for him going forward.

"When I say partnerships, I have to say that is not a word the government actually understands," Ware explained. "We have to form partnerships that work for both sides of the partnership, so to speak. That's really the culture we're building at CISA — it's a requirement we have to do the job that we're called upon to do."

Ware also predicted that the trend of CISA's focus (and DHS's focus, more broadly) on cybersecurity will continue in 2020.

"The critical infrastructure responsibilities that DHS has had since its formation have really morphed and evolved over time to be not just the physical risks that we used to be concerned about after 9/11, when DHS was formed, but now increasingly the cybersecurity risks to critical infrastructure," Ware said. CISA's cybersecurity directorate is moving to a focus on proactive threat hunting rather than reactive incident response and information sharing, he added.

When asked about "connecting data to security" Ware suggested flipping the topic, imagining security without data. It would be hard to gauge any policy or system's effectiveness without the data, and as data becomes an even more crucial part of all IT systems, he called for "securing the data itself," both at rest and in motion. It sounds like an easy proposition, and it is one that is commonly repeated throughout the security sector. As a newcomer, Ware added, he has a new "appreciation" for size of the challenge.

“Because of [the volume of data], it’s really hard to see things that are important,” Ware explained. “[Indicators of compromise] are increasingly having false positive rates, because as we’ve been able to collect and share indicators, our adversaries are changing their strategies and tactics.” CISA will have to step up its role sharing information, he said, in order to provide context to those indicators, which relies upon leveraging security data. In turn, that will require data to be accessible and verifiable.

Ware said he appreciated CISA’s adaptability in the past and looks forward to that same resiliency in the future.

“We think we know what we need five years from now,” he said. “But think about how many things, really, have changed in the last two years that we weren’t fully accounting for. Those programs … were designed like they were single-point solutions, and that target has moved significantly over the last few years. It creates an incredible pressure on the challenges of integrating data: how we move data from a silo for which it was designed into a place where it can be leveraged for new mission areas, [and] how we move across one specific vendor solution to multi-vendor solutions.”

Ware concluded by sharing some of the priorities CISA’s cybersecurity directorate has for 2020, including “embracing multi-cloud environments;” retiring legacy systems; “designing for scale [and] sharing,” which is especially difficult considering classification and privacy concerns; and “aligning across our mission areas,” to make the best use of past knowledge when combining it with emerging technologies like AI and machine learning.

View printer friendly version
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Federal Cybersecurity
data protection
Data Analytics
Standard