Homeland Security's New Approach to Cyberrisk Management

DHS is looking past information sharing to a complete cross-sector shared critical warning system for cyberthreat indicators.

Amanda Ziadeh

Fri, 06/15/2018 - 14:18

Illustration: traffic_analyzer/iStock

The Homeland Security Department is reassessing its cybersecurity risk strategy. Rather than thinking about the risk to assets and systems, it'll focus on the functions and services citizens rely on, and how to respond when those functions are threatened.

"We see ourselves as the national risk managers," said Jeanette Manfra, DHS' National Protection and Programs Directorate assistant secretary for the Office of Cybersecurity and Communications, at the June 14 Akamai Government Forum in

Washington, D.C.

The NPPD team is looking at its entire mission space, rethinking whether it’s doing the right things, deploying the right kinds of technologies and enforcing the right policies to protect the nation from cyberthreats.

Specifically, DHS has been given unique authorities in the federal government to, for example, direct federal agencies to take cybersecurity action, protect critical infrastructure information for release for a FOIA or regulatory purposes, to apply liability protections to companies sharing information through DHS, and so on, according to Manfra.

So, her team is working to build the capacity and capabilities to fully own those authorities in the federal civilian side and around how it supports critical infrastructure in order to support a more secure ecosystem.

Risk Strategy

Manfra said the DHS cybersecurity strategy takes the department back to its routes.

“We’re a risk management organization,” she said. Risk can’t be eliminated, so it has to be managed, and not just throughout the government, but nationally.

“Our organization is the one place that has the authorities and the capabilities to be able to take a step back and think about risk, and then what are those tools that we have to actually manage that risk?” Manfra said.

The first step is identifying risk — and not just in a segmented, every-agency-for-themselves way, but broadly. Thinking about cybersecurity risk federally typically means compliance, the Federal Information Security Management Act, authority to operate processes and checklists, Manfra said. Oftentimes, these compliance checklists aren’t directly connected to the agency’s mission risk.

So, as agencies continue to think about their risk, “we at DHS need to be understanding enterprise risk for the federal civilian enterprise. We can’t just think about each agency on its own,” Manfra said. Because as agencies move to modernization and cloud adoption, the federal space is becoming more connected. How well one department secures its database may have an impact on another department’s systems or network.

Rather than identifying which systems are most important based on the type of data they hold, “we have to connect those systems to the actual mission or business,” Manfra said, prioritizing mission-critical systems first.

National Critical Functions

For DHS, that means understanding national risk while agencies continue to adopt the cybersecurity framework and explore individual risk. Manfra referred to this new concept as national critical functions: functions citizens and the nation depend on.

This approach of rigorously thinking about what is critical to the nation’s functions hasn’t been done in a “long time,” Manfra explained, and hasn’t been done with the thought of IT dependencies on those functions.

So, DHS is working closely with industry to identify those functions, and rather than thinking about assets and systems, prioritizing the functions and services in times of disaster or crisis. There needs to be a mutual understanding between government and industry about what these are.

“I believe that starting there is really going to change the outputs of what we’ve previously been calling information sharing,” Manfra said. “Information sharing doesn’t quite capture what we really need to do.”

That is, there needs to be well-instrumented indicators of a warning system across the country between industry and government, Manfra said. Government, industry and the intelligence community need to understand what the national critical functions are and who owns the pieces of the functions.

This will create a collection of information on the potential for an adversary to disrupt those critical functions, and how to be alert and warn others of a threat. These warnings should span from broad, systematic-type risks and local risks to attacks like WannaCry.

Then, DHS can assess the risks to those functions, who owns that risk and identify the actual dependencies on a specific network, system or platform.

And it shouldn't just be government pushing out alerts through the U.S. Computer Emergency Readiness Team site, where people may not know which bulletins to pay attention to.

"It's about actually having an instrumented system that people know how to communicate with each other, and how to connect the dots very quickly," Manfra said.

This will require a change in the way government works, because it's a different type of national security situation. Industry is, for the most part, on the frontlines, and has most of the pieces and data the government needs to fully understand what's going on, Manfra said.

"We have a duty to warn and ensure that that [information] gets out," she added. In fact, as part of a broader collective defense model, those who participate in managing some aspects of those risks also have a duty to make sure other members of that ecosystem are aware of the situation.

Contingency Plan

But this doesn't mean DHS expects to predict every threat — in fact, Manfra knows it won't. So, how does DHS ensure the nation is well positioned with a contingency plan in place, or what the government, local and state organizations and industry are going to do if there is a significant incident?

It took time to develop federal emergency management plans, but "we need to do the same thing in cybersecurity," Manfra said. There needs to be clarity, roles and responsibilities around when and how departments will provide assistance, when FEMA is available, when the National Guard is available, and so on — because cyberthreats are not traditional emergency management concepts.

“If we don’t build that out and operationalize that, we’re going to get in situations where people are stepping on each other,” Manfra said, resulting in an even bigger issue.

So, DHS wants to get ahead of this, identify those functions, involve the proper stakeholders and start building those playbooks and contingency plans so that the government is ready to mitigate cyberattack consequences.

This new cybersecurity risk management strategy is something Manfra said the NPPD is going to be working on over the next couple of years, and she’s “very excited about that.”

View printer friendly version
Department of Homeland Security
Jeanette Manfra
Federal Cybersecurity
risk
cyberattacks