Why Cybersecurity is no Longer Just the CIO's Problem

As government agencies go digital, increased cyber risks require a holistic approach. Kate Macri
Fri, 07/17/2020 - 12:54

Cybersecurity officials want government agencies to prioritize two principles to maximize their cybersecurity effectiveness. First, cybersecurity is a team sport that requires cooperation with other departments within an agency as well as other agencies and private sector vendors. Second, continuous real-time visibility of all your assets is paramount to getting in front of cyber adversaries.

As government agencies become increasingly digitally connected, one organization’s best cybersecurity practices no longer affect just that organization.
“We have seen a significant teutonic shift in the landscape of stakeholders and the interconnectedness of our community right now,” said Daniel Kroese, associate director of the National Risk Management Center at the Cybersecurity and Infrastructure Security Agency (CISA), at an Electrosoft cybersecurity summit this week. “The transformation we're seeing right now really demands a whole of society and a whole of government approach going forward.”

Government needs to be aware of a “holistic cyber risk picture for the nation,” he added, because everyone — in both the public and private sectors — is connected to each other via software applications, clouds and the "internet of things."

“CISA has a unique perspective here,” he added. “We've got a .gov protection mission, and the second mission, which I focus more on, is our critical infrastructure vulnerability and resiliency mission. ... What that visibility has shown is this is no longer just about one company or one network. A static one-company worldview is not going to give you the holistic picture of the threat landscape.”

As all aspects of business digitize, they develop cyber risk that might not have existed before. Cybersecurity responsibility can no longer be assigned to one department, it must be addressed by all department heads in a federal agency, government contractor or private company.

Two key areas where cyber risk is exploding right now are supply chain management and infrastructure management.

“It's really hard to look at cyber risk in silos right now,” Kroese said. “It's becoming increasingly hard to disaggregate the disciplines of cyber risk management, supply chain management and critical infrastructure protection. They're all intertwined layers on top of each other. That's been a real shift for us over the past few years. We've really had to layer on this complicated interconnected understanding of how the nation's infrastructure operates and potential pinch points.”

For example, federal agencies need to consider their private-sector contractors as part of their risk management portfolio, said General Services Administration Cloud Acquisition Team Product Specialist Skip Jentsch.
After purchasing and installing cloud services, a government agency’s IT department must assess the new cloud infrastructure to make sure it meets government security standards. Then, the agency CIO signs off on the authority to operate (ATO).

But if the agency’s cloud is managed by the cloud services provider, then that provider must meet government ATO standards as well. The Federal Risk and Authorization Management Program (FedRAMP) streamlines this process.

“FedRAMP engages a third-party consultant to go one time with a clipboard to check off all the controls to see what the security posture of that cloud service provider is,” Jentsch said at the ATARC IT Acquisition Summit this week.

By working with contractors to ensure the right cybersecurity standards are in place, government agencies can gain better visibility and a deeper understanding of the risks and potential weaknesses in their cloud infrastructure.

“If a vendor offers a piece of software that an agency can't do without, they might go for that and help that vendor achieve a federal ATO and then that software can go into production,” Jentsch added.

As more agencies shift to cloud services and other software applications, they create more “commonality” and may unwittingly make it easier for criminals and nation-state actors to attack their networks. This is because the underpinning software and hardware building blocks of IT are very similar, Kroese said.

“If you look at the universe of information and communications technology, there's a lot of commonality in the attack surface across those connected underpinning building blocks of our digital infrastructure right now,” he said. “That increases the need to be extraordinarily vigilant."

One way federal agencies can do this is by participating in CISA’s Continuous Diagnostics and Mitigation (CDM) program.

Kevin Cox, CDM program manager at CISA, said agencies can maintain real-time visibility and monitoring of all the access points on their networks through the CDM Program and instantly see when something needs patched or when something is infiltrated.
“I think it's really very telling in regard to what we need to help [federal] agencies get a better handle on and better visibility of in regard to their overall network,” he said at an event hosted by MeriTalk this week. “The idea that what you don't know about you can't protect is a key aspect of it. First and foremost we want to make sure agencies have the broad visibility they need, not only their assets, but also their credentialed users, their private users, what their perimeter looks like, as well as what data they have out in the cloud and on mobile devices.”

CDM is all about monitoring every single access point — every smartphone, every laptop, every router — that has access to your network, which may include the private-sector contractor controlling your cloud services.

“For the agency to protect its full environment it needs to understand its full environment,” Cox said. “Every connection into an agency, every channel that gets to a piece of the agency's data is an avenue through which our adversaries can move into the agency network and exploit that data and potentially move laterally to exploit other data. Wherever there are vulnerabilities we have to assume they are utilizing those channels and vulnerabilities to get on the network.”

CISA exists to help federal agencies make sure their cybersecurity posture is in good shape, Cox added.

“The state of cybersecurity risk management right now is more than just 'patching your stuff,' that's a baseline expectation,” Kroese said. “Cybersecurity is a team sport. It takes the executive branch, Capitol Hill, industry, academia.”