FCW Cybersecurity Summit

Sponsored by IBM

Cyberthreat Intelligence Helps Augment Protection

CDM can go a long way toward tracking assets, but it falls short when it comes to the cloud, mobility, and human factors.

Cyberthreat intelligence entails many things, such as understanding your infrastructure, your employees and your information, but the bottom line is it provides actionable information, say experts during a recent fireside chat program entitled "Intelligence-Driven Security."

"The key here is really the insight for action," says Shue-Jane Thompson, vice president and partner of IBM's Cybersecurity and Biometrics Division. "How do you gain the insight—prioritize and filter in the insight—so then you can allocate your resources for appropriate action? Know you don't know, and know better of the part you already know."

Darryl Peek, director of operations at the Office of the Homeland Security Chief Information Officer and Chief Technology Officer, says he associates cyberthreat intelligence with National Institute of Standards and Technology's Special Publication 800-50, which defines a cyberthreat as something that could potentially affect an organization, individual, or nation using adversarial techniques. "The intelligence part of it is the sharing of information in regard to that potential threat and making sure that all aspects of your environment are benefitting from the information and the resolution of that," says Peek.

The Continuous Diagnostics and Mitigation (CDM) program is taking steps toward giving federal agencies better situational awareness, but the initial blanket-purchase agreement omitted two things, says Peek: cloud and mobile. "Realizing that a modern workforce is a mobile workforce, that now has to be considered as an important priority for the program, and I know that there are steps being made in order to address that."

Those steps are actively underway. "We are going through a period of IT modernization," he says. Agencies are shifting to software-defined networks, cloud, and block-chain infrastructures, for example. Some are looking at using containerization and micro services. Securing those becomes another issue.

CDM also doesn't take human beings into account. For instance, phishing attacks are still one of the most-used tactics. Education, awareness, and training can help here, but go beyond traditional manuals and use gaming or simulations to get employees to really pay attention, says Thompson. "The human factor is really the core of cybersecurity incidents."

Another shortfall associated with CDM is a deficit of workers required to sift through the petabytes and exabytes of data the identify, detect, and protect steps generate. By 2021, 3.5 million cybersecurity jobs will be available, according to Cybersecurity Ventures. "Human intelligence is no longer sufficient," says Thompson. "We're going to lean on machine learning. We're going to lean on the cognitive technologies so we'll be able to stay ahead of the threat intelligence."

Agencies need to track not only shortcomings, but also successes, says the experts. Thompson recommends using metrics to study repeated threats or incidents, which indicates a gap in cybersecurity, and studying the number and trends of preventable threats that got through. "If you have not done your prevention, probably the threat intelligence analysis has not done a very good job."

> "We are going through a period of **IT modernization**."
>
> **DARRYL PEEK,**
> DIRECTOR OF OPERATIONS AT THE OFFICE OF THE HOMELAND SECURITY CHIEF INFORMATION OFFICER AND CHIEF TECHNOLOGY OFFICER

She also recommends measuring the time between threat detection and recovery, as well as the degree of impact attacks have on the organization. For example, DHS measures itself against Federal Information Security Management Act annual reports to track its progress in gaining situational awareness.

Metrics should be part of agencies' cyberhygiene, says Thompson. She says the next layer is using cyberintelligence to augment, orchestrate, and automate cybersecurity operations. The top layer is cyberresilience. Multiple agencies can operate under a single policy so they can easily share intelligence and resources.

"Without a fundamental data structure and model, we cannot communicate across the agencies, let alone we want to do enterprise levels of communication," says Thompson. "To me, in cybersecurity, it's not big data only, it's mega data."