DoIT's OSM Summit Brings Awareness to Current Cyber Training Services

February 15, 2023

Article and Photos by Chazz Kibler

John Bruns addresses the room with opening remarks.

CROWNSVILLE, Md. - The Maryland Department of Information Technology Office of Security Management hosted various state agencies and municipalities for the Security Awareness Training Summit here on Feb. 15, 2023. The summit intends to bring awareness to the current service, the importance of remaining engaged in the program, and the agencies' expectations regarding awareness training. Some discussion topics included role-based training, quarterly service reviews, monthly awareness training, and more.

“Leading the [summit] was good,” said Jacob Chandler, senior cyber training manager with DoIT’s OSM team. “Our goal is to drive up completion rates by having folks actually going into that portal and taking that training, which shows us success.”

Andrew Neboshynsky, left, converses with Jacob Chandler during a break.

For those in attendance, either in person or virtually, the summit provided agency representatives a chance to expand or refresh their cybersecurity knowledge, understand upcoming service improvements and expectations, and network with agency counterparts on these topics.

“With an administration change in the state, we had a chance here to reinvent what we’re doing and get a new energy behind us,” said Andrew Neboshynsky, the chief information security officer with the Maryland State Department of Education. “It’s good to hear that the training program here at DoIT wants input from the people getting the training.”

The expectation is for the agency’s key stakeholders and security awareness training managers to understand the progress that should occur with awareness training in the state and to engage with OSM to help make improvements within their organizations.

“So, what we were doing here today was really geared towards a lot of our trainers,” said Donnie Green, director of cybersecurity operations at DoIT.

Donnie Green, center, talks to two attendees following the summit's conclusion.

“We did talk about our quarterly service reviews, and in that, we want to get more of the trainer and the executive-level personnel involved in those meetings because what we need is that buy-in.”

Part of that “buy-in” involves agencies using DoIT’s available services, such as our simulated phishing program, which sends simulated phishing emails to employees to gauge their awareness of attacks and what to do with phishing emails when they receive them.

Jacob Chandler fields questions from the audience.

“The intention of actually running a phishing campaign is not to trick folks,” said Chandler. “It’s actually intended to bring awareness to what an inappropriate email might look like.”

Chandler’s role in cybersecurity awareness training doesn’t begin and end at cybersecurity training sessions; he also makes it a priority to make himself available to address any questions, comments, or concerns agencies may have regarding this service.

The Security Services team provides State agencies with a common statewide strategy for secure, effective, and technically sound use of the State's information technology resources. To learn more about our cybersecurity services, click here.