STATE AFFAIRS
WISPOLITICS
Wisconsin's Premier Political News Service

WI National Guard: Wisconsin Guard unit part of first DHS/CISA cyber tabletop exercise at university

Posted on Monday, Nov 14, 2022

MADISON, Wis. — Approximately 75 University of Wisconsin-Madison computer science students watched Patrick Skufca, a Cybersecurity and Infrastructure Security Agency (CISA) exercise facilitator, slowly pace around the university's Union South Varsity Hall Ballroom, the echo of his footsteps punctuating his questions.

Skufca asked students to define a cyberattack. He asked them to identify recent cyberattacks in the news. He then polled students on the biggest targets of cyber attackers. Answers ranged from small, independent businesses to large companies with deep pockets, infrastructure such as energy or water utilities, banks — even government contractors.

"Everyone is a possible target," Skufca said. "It's up to everyone to be cyber-resilient."

Skufca was part of a Department of Homeland Security and CISA developed and facilitated tabletop exercise at the university Nov. 3 that included representatives from the University of Wisconsin, the city of Madison water utility, the Milwaukee office of the Federal Bureau of Investigation, and the Wisconsin National Guard's Detachment 1, 176th Cyber Protection Team.

This was the first cyber tabletop exercise DHS and CISA have conducted at an academic institution, according to 1st Lt. David Schroeder, cyber defense manager with Detachment 1, 176th Cyber Protection Team, and program manager for the Wisconsin Federated Cyber Program. The students were enrolled in Prof. Bart

Miller’s computer science software security program.

“Prof. Miller wanted participation from other partners, such as FBI cyber, the Madison Water Utility and the Wisconsin National Guard,” Schroeder said, “to add more realism and expertise to the event and also to create a partnership between UW-Madison and the Wisconsin National Guard.”

Schroeder is already familiar with Miller, a Vilas Distinguished Achievement Professor and the Amar and Belinder Sohi Professor of Computer Sciences at UW-Madison.

“I am also the national security research strategist for the School of Computer, Data and Information Sciences at UW-Madison,” Schroeder said. “I have worked with Bart for many years.”

UW-Madison is a founding member of the new U.S. Cyber Command Academic Engagement network, and the 176th Cyber Protection Team is part of the Cyber Mission Force — U.S. Cyber Command’s action arm which directs, synchronizes and coordinates cyberspace operations in defense of the nation’s interests. The tabletop exercise provided visibility to students about the kinds of cyber roles, responsibilities and opportunities available in the Wisconsin National Guard and the military in general. The exercise also touched on topics that aligned with the cyber protection team’s training requirements.

The next day, Nov. 4, Miller spoke about the ransomware landscape to personnel at the Wisconsin National Guard’s Joint Force Headquarters in Madison in what was billed as the first of a planned annual cyber tech talk.

Miller said the mission of cyber defenders is to anticipate threats, demonstrate the feasibility of those threats and to defend against those strategies.

“Our job is to stay ahead of attackers as best we can,” Miller said.

To defend against ransomware — cyberattacks that steal information or deny access to software or files, then demand money to resolve the matter — Miller outlined certain goals, such as developing a comprehensive understanding of how ransomware exploits systems, developing strategies to minimize damage, and develop strategies to automate recovery after an attack.

“You will be hacked — so now what?” Miller asked. Detection and recovery strategies are key to being resilient during a ransomware attack.

Miller said that most ransomware perpetrators tend to be honest business people, in the sense that they want their victims to pay the demanded ransoms, so the victims need to trust that paying the ransom will end the attack.

“Most hackers aren’t warriors — they’re weenies,” Miller said.

After the ransomware presentation, Miller and the Cyber Protection Team reconvened in the Wisconsin Cyber and Intelligence Center, along with members of the Wisconsin National Guard’s Defensive Cyber Operations Element (DCOE) and Cyber Response Team (CRT), for a technical talk delving into Miller’s work on malware reverse engineering, used to understand the inner workings of newly-discovered malware.

Schroeder said the exercise and Miller’s presentations the following day constitute continuing education units for Cyber Protection Team personnel, which can be used to fulfill training requirements.

The 176th Cyber Protection Team formed in 2017 with detachments in Illinois and Wisconsin. The unit deployed to Fort Meade, Md., in October 2020 for a 14-month mission in support of U.S. Cyber Command.