STATE AFFAIRS
WISPOLITICS
Wisconsin's Premier Political News Service

Dept. of Military Affairs: Annual cyber security summit focuses on protecting critical infrastructure

Posted on Friday, Oct 27, 2017

CONTACT: Jackie Guthrie | ngwi.pao@mail.mil | 608-242-3050

By Sgt. Katie Eggers

MADISON, Wis. — More than 350 government, business, and academic leaders gathered recently at the fifth Annual Governor's Cybersecurity Summit, to exchange knowledge and experiences in the ongoing effort to secure our states digital infrastructure.

Nationally recognized cyber security experts participated at the October 16 Cyber Security Summit held at the University of Wisconsin. They discussed issues facing the industry, which included a shortage of cyber security experts, to the National Guard's role in developing cyber response teams.

The annual summit is held in conjunction with Wisconsin's Cyber Security Awareness Month campaign. Gov. Scott Walker issues the annual proclamation to recognize and acknowledge the vital role Wisconsin has in identifying, protecting, detecting, responding to and recovering from cyber threats to the state's critical infrastructure and to encourage citizens to take appropriate steps to protect their information.

Protecting critical infrastructure is very easy to talk about, but hard to do, Maj. Gen. Don Dunbar, Wisconsin's adjutant general and homeland security advisor told attendees at the fifth annual summit that took place at the University of Wisconsin and shared some of the state's efforts.

“We have developed five cyber response teams here in the state of Wisconsin,” Dunbar said. “Three of them are state and local government allowing their IT professionals to train together, and then if something happens we can respond as a team. The National Guard is filling a fourth team, and we’re working with our industry partners to form a fifth team.”

Dunbar added that a current challenge facing cyber response is the reluctance for organizations to share information that could be important when protecting and securing critical infrastructure.

Frank Grimmelmann, the president and CEO of the Arizona Cyber Threat Response Alliance (ACTRA), agreed and spoke about ACTRA’s 1,800 private sector and government partners they have working together sharing vital information. He told participants that ACTRA is assisting Wisconsin in building a similar network, the Wisconsin Cyber Threat Response Alliance, or WICTRA.

“What we are doing is replicating the essential components that will be essential to the state of Wisconsin that will allow you to, from the grassroots level, put in place something that works for you, and something that, working together, will raise the bar for both of us,” Grimmelman said.

Presenters also discussed a different challenge facing cyber security – the lack of cybersecurity professionals. Small businesses to major corporations are competing for well-trained cyber professionals.

“This problem of cyber manpower is so bad right now, that the country is actually starting to look abroad [to see what other countries are doing],” said Allan Paller, founder of the SANS Insitute, and organization that specializes in information security training and cyber security.

Paller told participants how other states and nations are developing tests and training courses to identify and recruit cyber talent to begin building a pipeline of cyber security professionals.

When it comes to the National Guard, IT professionals don’t necessarily have to choose between serving their country and working for a high-paying IT company. That’s according to Col. Kelly Hughes, the senior cyber advisor to the Joint Force Command of the Washington National Guard.

“They’re not here for the money,” Hughes said. “It was the types of missions that they were doing, that they could serve their country and then take their skills and help us out.”

Another challenge facing the industry is getting the public to embrace cyber awareness. Despite all the security systems developed and implemented, if the consumer doesn’t use them, they are worthless, said Dr. Jen Golbeck, a leader on social media and online communication.

“From the beginning, security has been designed without making people part of the system,” Golbeck said.

Many rules set to define a secure password make the password impossible for humans to remember. There is a stigma that if security systems are easier for users, such as using biometrics to log onto a phone, the system is less secure.

“Human beings cannot be upgraded,” Golbeck said. “We come with a set of social, cognitive, psychological capabilities and limitations, and you can’t change those.”

In addition, people generally try to be nice – letting others borrow a computer, granting them access to their network, she said. She challenged security professionals in the audience to figure out how to make “the nice thing the most secure thing to do.”