Equifax breach brings renewed attention to information security vulnerabilities

September 20 2017, by Saralyn Lyons

The recent Equifax breach, which compromised the personal data of more than 143 million American consumers, was a frequent topic of conversation during the fourth annual Cyber Security Conference held Tuesday at Johns Hopkins University. It topped conference organizer Anton Dahbura's "Unlucky 13" list of cyber concerns that have come to light in the past two weeks.

Yes—that's 13 concerns in two weeks.

"This is becoming quite an issue because of its scale," said Dahbura, executive director of the Information Security Institute, which co-hosted the conference along with Compass Cyber Security. "Now is the time to talk seriously about a national identification system. ... We need an ID solution for the 21st century. Enough is enough."

Despite the clear need for new approaches to information security, the industry and government experts who spoke at the conference also identified barriers to improved security.

"On a daily basis, we have more than 300 terabytes of data going in and out of the Department of Defense," said retired Brig. Gen. Guy Walsh, who serves as adviser to the deputy commander for U.S. Cyber Command.

He said that only last month did the U.S. government separate Cyber Command out from under the National Security Agency to make it its

own unified command capable of setting its own agenda and priorities. Cyber is now considered the fifth operational domain for warfare, along with land, sea, air, and space.

Walsh underscored the importance of recruiting IT professionals and white hat hackers for the military's efforts to combat cyber attacks.

"We have this huge, interconnected world at war," he said. "Our next Pearl Harbor will be cyber-related."

The conference speakers also emphasized the role private industry plays in cybersecurity. Health care, in particular, has become a prominent target for certain types of attacks, said Stephanie Reel, chief information officer at Johns Hopkins. Ransomware, an attack that holds information and computer systems hostage until a fee is paid, particularly affects health systems because of the sensitivity of the data that's compromised and the urgency with which patient medical records must be recovered in order for the facility to operate normally.

Ultimately, there is a lack of accountability in industries that collect personally identifiable information. As data breaches increase in frequency and in the number of people affected, the need for more regulation—or better regulation—will be a focus, said Byron Patrick, managing director of the CPA practice at Network Alliance.

"There is hardly ever a regulation put in place before a building burns down," he said. "We need to be more proactive and less responsive, or there are going to be a lot of burning buildings, like Equifax, before we get the regulations we need."

Provided by Johns Hopkins University