SNL Blogs

Wednesday, October 01, 2014 6:44 PM ET

Cybersecurity is the new black

By Daniel Young

Government officials and industry observers discussed the impact of cybersecurity threats at *The Washington Post*'s Cybersecurity Summit on Oct. 1.

Rep. Mike Rogers, R-Mich., said that contrary to popular belief regarding the Internet, the NSA does not monitor 85% of the public network, only the 15% directly under government control. However, it was that public part of the Internet which was vulnerable in recent attacks aimed at the financial sector. "It's that 85% of the public networks [that] will not be ready for what comes next," he added.

Rogers explained that state actors, such as Iran and Russia, have tried to infiltrate U.S. financial systems. Iran, he said, has probed the financial industry to destroy data. They are using cyberthreats as a political tool, he added. Rogers is chairman of the House Intelligence Committee.

Sanctions placed on Russia have prompted bad actors to try to infiltrate the U.S. financial environment in an effort to "disrupt the economic fabric" of the U.S., according to Rogers. He said it is hard to determine if the threat comes from hackers or the state but that the sanctions are behind the intent of the intrusions.

"Our noses are just above the water," Rogers said of the efforts to keep ahead of cybersecurity threats.

"We, as a nation and many countries in the world, have put almost everything we value in cyberspace," said panelist John Carlin, who is assistant attorney general for national security at the Department of Justice. "We put our personal information, our financial information, we put the way we operate our critical infrastructure, digitally stored, and most of it is connected to the Internet."

Carlin added, "The bad guys are going where the money is, where the secrets are and where they can cause the damage."

That damage is inflicted by one of four types of players, according to Eric Friedberg, executive chairman of Stroz Friedberg. There are those looking to steal intellectual property, those looking to steal financial information, "hactavist" players looking to cause embarrassment for businesses, and corrupt or negligent corporate insiders.

Carlin said the damages include a loss of over $300 billion in intellectual property as a result of data breaches. The amount of that loss does not include the damage done when data breaches occur, such as in the case with Target and Home Depot. These large-scale breaches add more than just the cost of card replacement and credit monitoring services. Friedberg said that "hard costs" can be in the range of $5 million to $20 million per incident and the "reputational costs can run into the hundreds of millions of dollars."

Friedberg added that the situation has gotten worse because the attacks have gotten enormous. "The top has to own cybersecurity threats," Friedberg said. There has to be corporate governance around security, he said, and there has to be a commitment to the technology.

"It's a cat-and-mouse game, where companies are often playing catch up," he added.

Yet, according to Christopher Painter, coordinator of cyber issues at the State Department, executives are already on top of it. "The awareness of cyberthreats is now at the highest level within corporations like we've never seen before," he said, adding, "Cybersecurity is the new black."

As the Internet enters its "teenage period," said Arati Prabhakar, the director of Defense Advanced Research Projects Agency, "it's time to tame the unruly teenager."