Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

The Weekly Newsletter of The George Washington University Cyber Security Policy and Research Institute

Quick Links

About CSPRI

Contact Us

Newsletter Archive

Blog: The CSPRI Byte

Follow Us

Follow us on Twitter:
@gwCSPRI

Follow CSPRI Director, Lance Hoffman:
@lancehoffman1

Follow CSPRI Associate Director, Costis Toregas:
@DrCostisToregas

November 9, 2015

Six (6) events scheduled in the Greater Washington Area in the next few weeks.

Legislative Lowdown

-The U.S. Senate late last month approved the Cyber Security Information Sharing Act (CISA), a bill designed to help companies share cyber threat information among themselves and with the federal government without having to worry about getting sued for doing so. But the bill has attracted significant opposition from the technology industry and from privacy advocates. Forbes breaks down the opposition to CISA, and its prospects in the House.

Cyber Security Policy News

New White House plan on cybersecurity
-The Obama administration last week issued a broad new plan designed to better respond to cybersecurity incidents such as those that exposed secrets on millions of citizens as well as government operations, according to NextGov. "The new guidance, which aims to protect the most high-value information assets the federal government holds, is the latest step in the months-long fallout from the devastating hack of sensitive federal employee files from the Office of Personnel Management revealed this summer," write Aliya Sternstein and Jack Moore.

Events

November 10
Responding to Looming Cyber Threats

November 10
National Security and the Cyber Threat Landscape

November 10
FedCyber 2015 Annual Summit

November 18
ISACA NCA Meetup: Conference on treads in mobile computing

November 18
ISSA Baltimore Meetup: Advanced endpoint protection

November 18
NovaInfosec Meetup West

Click here for detailed descriptions

US Cyber Command update
Sternstein also writes about another, more eyebrow-raising development: The U.S. Cyber Command has put forth nearly a half-billion dollar contract for computer code capable of killing adversaries. "U.S. troops would have the power to launch logic bombs, instead of traditional explosive projectiles, which essentially would direct an enemy's critical infrastructure to self-destruct," Sternstein writes. "Lethal cyber weapons have arrived." Read more here.

Cox Communications update
-The Federal Communications Commission last week fined cable giant Cox Communications nearly $600,000 for failing to better secure their corporate network from outsiders. In 2014, hackers associated with the cybercrime gang the Lizard Squad tricked two different Cox employees into clicking on link to a fake site, stealing credentials that allowed the fraudster to pull Social Security numbers, drivers license information and other sensitive data on several dozen customers, including security journalist Brian Krebs, who wrote about the ordeal and what it says about ISP security in general. The case is widely seen as a first for the FCC, and an indication that the agency intends to be more active in policing corporate cybersecurity.

Trans-Pacific Partnership (TPP): the pending impact on cybersecurity
-The Trans-Pacific Partnership (TPP) trade deal could have a big impact on cybersecurity, writes Stewart Baker for The Washington Post. "That's because the deal prohibits nations from asking mass market software companies for access to their source code," Baker explains. "The ban doesn't apply to code run on critical infrastructure, which will make for endless disputes, since there's very little mass market software that doesn't run on computers involved in critical infrastructure."

Communication efficiency test between US and UK government & financial entities
A coordinated simulation to test how well the United States' and United Kingdom's government agencies and financial centers in London and New York communicate in the event of a cyberattack on the financial sector will take place this month, officials stated today, DarkReading reports. "The joint exercise is the result of a set of agreements for cybersecurity cooperation laid out by President Obama and U.K. Prime Minister David Cameron in January," Sarah Peters reports.

NIST asking for feedback to better security frameworks
If you know mobile security, the National Institute of Standards and Technology (NIST) wants your help. "Government scientists are asking for feedback on a new guide they've developed to help companies establish a secure framework for their employees'

mobile devices - increasingly a key component of business models around the country," writesGrayson Ullman for FedScoop. "NIST mapped out a number of potential vulnerabilities, including email and calendar apps, and compiled commercially available cybersecurity software to counter them. The guide includes instructions on how to install software and remove sensitive information when an employee leaves an organization."

About this Newsletter

This newsletter is a weekly summary of events related to cyber security policy and research, with a special focus on developments and events in the Washington, DC area. It is published by the Cyber Security Policy and Research Institute (CSPRI) of the George Washington University. CSPRI is a center for GW and the Washington area that promotes technical research and policy analysis of topics in or related to cybersecurity. More information is available at our website, http://www.cspri.seas.gwu.edu

CSPRI

202 994 5613, **cspri@gwu.edu**
Tompkins Hall, Suite 106
725 23rd Street NW
Washington DC, DC 20052