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

September 8, 2015

Nine (9) events scheduled in the Greater Washington Area in the next few weeks.

New CSPRI Report

The new CSPRI report, "A New Privacy Framework with Criteria Inspired by Fair Information Practice Principles" introduces a new framework that uses the FIPPs to develop a criteria-based approach for assessing and evaluating policies and practices and ultimately comparing information systems.

Read the report **here.**

Legislative Lowdown

-With Congress returning from its summer recess, a cybersecurity information-sharing bill that stalled earlier this summer is competing for lawmakers' attention with debates over the president's nuclear deal with Iran and the looming budget deadline, according to National Journal. "Opponents of Cybersecurity Information Sharing Act -tech experts, privacy advocates, and pro-privacy lawmakers- have fought to delay the bill and would rather see it dropped completely," writes Kaveh Waddell. "But if CISA does get buried under the Senate's packed schedule, experts say there are alternatives for lawmakers looking for ways to improve cybersecurity through legislation."

Events

September 9-10
Intelligence and National Security Summit

September 9-11
2015 Cybersecurity Innovation Forum

September 10
Worldwide Cyber Threats

September 10
Managing Cyber Risk and the Role of Insurance

September 10
Cyber 6.0

September 10
Senior Executive Cyber Security Conference

September 14-16
EnergySec Security and Compliance

September 16
GW Cyber Academy Open House

September 17
6th Annual Billington Cybersecurity Summit

-The auto industry is fighting back with a lobbying push to head off proposed new cybersecurity standards for carmakers in the wake of revelations that many modern communications systems in cars lends certain models to remote control and hacking. Politico writes that Sens. Edward Markey and Richard Blumenthal are gearing up to possibly offer their legislation as an amendment to a long-term transportation bill in October. Read more here.

Click here for detailed descriptions

Cyber Security Policy News

StingRay Update

-The Hill reports that the Justice Department last week unveiled new privacy protections for controversial devices that mimic cellphone towers and allow the government to warrantlessly identify people and determine their location. "Under a new policy, government agents will have to obtain a warrant before using the devices, known as StingRays, and routinely delete the information they pick up," writes Julian Hattem. "Additionally, the government will be banned from picking up people's emails, photos or other communications for criminal investigations, and officials will have to undergo audits to make sure they are complying with the rules."

US sanctions on China

-China's Ambassador to the United States Cui Tiankai said last week he doesn't believe reports of planned U.S. economic sanctions on Chinese companies and individuals involved in alleged cyber thefts from U.S. companies. "Cui said he hoped that 'nobody will do anything so nonconstructive,' and that he hoped 'the U.S. side will make the smart choice,' implying that economic sanctions would be the wrong choice," writes Lisa Brownlee at Forbes. "It was reported last Thursday that the U.S. would announce this week after today's Labor Day holiday economic sanctions against Chinese companies for cyber espionage on U.S. companies, rather than announce them later this month, as had been reported."

Jeep Cherokee Hack: Update

-Six weeks after hackers revealed vulnerabilities in a 2014 Jeep Cherokee that they could use to take over its transmission and brakes, Chrysler has pushed out its patch for that exploit. But the company is coming under another round of criticism for what some are calling a sloppy method of distributing that patch: On more than a million USB drives mailed to drivers via the US Postal Service. Andy Greenberg writes for Wired.com that Chrysler's response ignores years of security advice. "Security pros have long warned computer users not to plug in USB sticks sent to them in the mail-just as they shouldn't plug in thumb drives given to them by strangers or found in their company's parking lot-for fear that they could be

part of a mass malware mailing campaign," Greenbergreports. "Now Chrysler is asking consumers to do exactly that, potentially paving the way for a future attacker to spoof the USB mailers and trick users into installing malware on their cars or trucks."

Uber hires security researchers
Meanwhile, car-hailing service Uber has snatched up the two security researchers who exposed the auto industry cybersecurity failings. Reuters reports that Charlie Miller, who had been working at Twitter Inc, and Chris Valasek, who worked at security firm IOActive, have resigned from their jobs and will join Uber next week. "Miller and Valasek won wide attention this month after demonstrating that they could hack into a moving Jeep," according to Joe Menn and Heather Somerville. "An Uber spokeswoman said Miller and Valasek will work with the company's top security officers'to continue building out a world-class safety and security program at Uber.'"

United States v. Microsoft
-On September 9th, the Second Circuit Court of Appeals will hear a case with global business, technology, and legal implications. The case, *United States v. Microsoft,* presents a deceptively simple question: What's a multinational company to do when it receives a U.S. court order to turn over customer emails that are stored on a server in a foreign country and that may be subject to different data privacy laws? Datasecuritylaw.com has the lowdown on what's at stake in this case.

OPM Update
-The Office of Personnel Management (OPM) has awarded a $133 million contract to a private firm in an effort to provide credit monitoring services for three years to nearly 22 million people who had their Social Security numbers and other sensitive data stolen by cybercriminals. But security expert Brian Krebs writes that perhaps the agency should be offering the option to pay for the cost that victims may incur in "freezing" their credit files, a much more effective way of preventing identity theft. "Identity protection services like those offered by CSID, Experian and others do little to block identity theft: The most you can hope for from these services is that they will notify you after crooks have opened a new line of credit in your name," Krebs writes. "Where these services do excel is in helping with the time-consuming and expensive process of cleaning up your credit report with the major credit reporting agencies. The only step that will reliably block identity thieves from accessing your credit file - and therefore applying for new loans, credit cards and otherwise ruining your good name - is freezing your credit file with the major credit bureaus. But there's a catch: Depending on the state in which you reside, the freeze can cost $5 to $15 per credit bureau. Also, in some states consumers can be charged a fee to

temporarily lift the freeze." Read more here.

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