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 14, 2015

Eleven (11) events scheduled in the Greater Washington Area in the next few weeks.

Legislative Lowdown

-Competing bills that would reform the decades old Electronic Communications Privacy Act (ECPA) have gone nowhere in the past several years, and Congress faces a tough slog this year in making progress on the issue, reports The Hill. "And the most popular proposal, which has gained support from more than 300 congressmen and senators, does not even address Microsoft's concerns about the geographical limits of a U.S. warrant," writes Mario Trujillo. "Microsoft and other tech companies back a bill that would set limits on what kind of information the government can force a U.S. company to hand over when that data is stored overseas. The bill would not force a company to turn over data, even under a warrant, if the data concerns foreign citizens." See more on this topic in Cyber Security Policy News, below.

-The National Journal has the lowdown on the challenges in store for proponents of the Cybersecurity Information Sharing Act, a controversial bill that now has some 22 amendments that need to be considered in a busy time for lawmakers focused on appropriations. "The information-sharing bill and its amendments have pitted privacy advocates and security experts against businesses," The Journal reports. "Privacy advocates say the bill could result in

Events

September 14-16
EnergySec Security and Compliance

September 15-16
Borderless Cyber 2015

September 15
ISSA DC Meetup

September 16
Reforming the Electronic Communications Privacy Act

September 16
GW Cyber Academy Open House

September 16
ISSA Baltimore Meetup

September 16
NovaInfosec Meetup West

September 17
6th Annual Billington Cybersecurity Summit

September 17
CharmSec Meetup

companies improperly sharing individuals' sensitive personal information with the government-including law-enforcement and surveillance agencies-and they are lobbying for the Senate to drop CISA. Tech experts say there are more effective ways to improve cybersecurity than information-sharing."

Cyber Security Policy News

Big tech companies experiencing problems
-Multiple legal conflicts between federal investigators and Microsoft and Apple, reflect heightened corporate resistance, in the post-Edward J. Snowden era, by American technology companies intent on demonstrating that they are trying to protect customer information, according to The New York Times. Both tech companies are embroiled in legal tussles with the U.S. Justice Department; in Apple's case, DOJ officials advocate taking Apple to court over its refusal to comply with a court order to turn over, in real time, text messages between suspects using its iPhones. Apple replied that its system is set up so that this is not even possible for the company to comply. Likewise, Microsoft is set to go to trial this week in a case "being closely watched by industry officials and civil liberties advocates, began when the company refused to comply with a warrant in December 2013 for emails from a drug trafficking suspect," The Times wrote. "Microsoft said federal officials would have to get an order from an Irish court, because the emails were stored on servers in Dublin."

If the government prevails in its legal battle to compel Microsoft to turn over e-mails held on a server in Ireland, an "international firestorm" could result, an attorney for the tech giant told a federal court in New York on Wednesday. Washingtonpost.com's Ellen Nakashima has more on this angle.

DOJ: Wanting companies to weaken encryption
Meanwhile, the DOJ is on embarked on something akin to a charm offensive to win broader support for its claim that companies like Apple, Google and Microsoft should weaken security and encryption on their products to enable and respond to court-ordered wiretaps. "Playing down a narrative of an ongoing "crypto-war" between the government and the private sector, FBI Director James Comey said Thursday that shared security values between the two groups mean they should be working together," reports Kaveh Waddell for National Journal. "But Comey said the source of the tension between tech companies and Federal law enforcement - the proliferation of strong encryption standards that make it difficult or impossible to read intercepted communications-could be addressed if only the business community made a real effort to develop new encryption technologies."

September 23
Meritalk: CSX Cyber Security Brainstorm

October 1
Cybersecurity Summit

Click here for detailed descriptions

Department of Homeland Security: Update
-Officials with the Department of Homeland Security are offering some counterintuitive advice to agency cyber defenders: Leave hackers in their systems until outside investigators are called in, and close all federal data centers. "These might seem like drastic recommendations -- but they come from the mouths of a top Department of Homeland Security director and a recently departed DHS senior official, respectively," writes Aliya Sternstein for NextGov. "The compromise of secrets on 21.5 million national security personnel and their families in the care of the Office of Personnel Management exposed cyber shortcomings governmentwide that cannot be repaired overnight. Those failures include maintaining sensitive data on outdated machines and throwing out key evidence of a hack."

The advice comes amid new reports showing that cyber attackers successfully compromised the security of U.S. Department of Energy computer systems more than 150 times between 2010 and 2014. USA Today writes that "incident reports submitted by federal officials and contractors since late 2010 to the Energy Department's Joint Cybersecurity Coordination Center shows a near-consistent barrage of attempts to breach the security of critical information systems that contain sensitive data about the nation's power grid, nuclear weapons stockpile and energy labs."

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