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

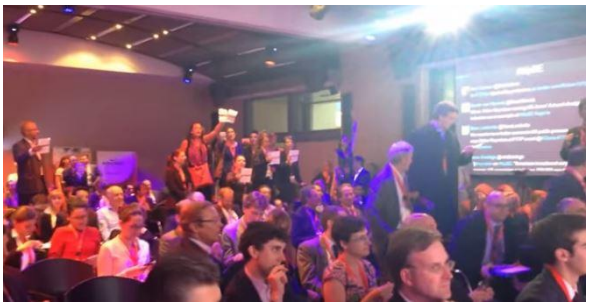
Follow CSPRI Director, Lance Hoffman: @lancehoffman1

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

July 6, 2015

Seven (7) Cyber security events are scheduled in the Greater Washington Area in the next few weeks.

Flash Mobs Next for Cybersecurity Conferences?



Flashmob choir interrupts TTIP congress.

Boingboing reports that a flash mob appeared last week at a congress where the Belgian Foreign Affairs Minister was promoting the Transatlantic Trade and Investment Partnership, a treaty described by some as a cousin to the controversial Trans Pacific Partnership. The flashmob of attendees stood up singly and then in bunches, singing "Do You Hear the People Sing?" a rousing revolutionary song from Les Miserables. See the video here.

Events

July 8

Securing .Gov

OPM Breach: tip of the iceberg?

Cyber Crime: Modernizing Our Legal Framework for the Information Age

FBI: The role of technology and the challenges of "going dark"

July 9

iOS authentication methods

NovaInfosec Meetup (West)

National Insider Threat Special Interest Group

Click here for detailed descriptions

As society sorts out the rules of the road for cybersecurity and for the Internet in general, some speculate that we may see similar uprisings at meetings of the IETF, ICANN, the Internet Society and other "rulemaking" bodies, official and unofficial, or at industry meetings such as Blackhat or RSA, or even professional society meetings such as those of the ACM or IEEE or IAPP.

Legislative Lowdown

-According to the Electronic Privacy Information Center (EPIC), several states have recently enacted new privacy laws. From their policy updates page: "New Hampshire and Oregonpassed student privacy legislation modeled after California'sStudent Online Personal Information Protection Act. Rhode Island and Connecticut enacted new consumer privacy anddata breach notification laws. A new Minnesota law limits the data police may capture using automated license plate readers and requires the deletion of all data not relevant to an investigation. And the Freedom from Unwanted Surveillance Act, a law in Florida regulating the commercial use of drones went into force this week. EPIC's State Policy Project is monitoring privacy bills nationwide."

Cyber Security Policy News

NSA update
-A federal court ruled last week that the National Security Agency can resume the bulk collection of American's phone records for roughly five months until the program is phased out. The ruling, documented by the National Journal, observes that "the Foreign Intelligence Surveillance Court approved a government request to renew the dragnet collection of U.S. phone metadata for an additional five months-a timeframe allowed under the Freedom Act, a newly enacted surveillance reform law that calls for an eventual end to the mass spying program exposed by Edward Snowden two years ago."

Meanwhile, CNN reports about investigations in Germany that indicate the NSA not only spied on journalists in that country, but also interfered in the exercise of the free press under the guise of U.S. national security. "That the NSA was spying on German officials is not new, though it continues to upset free press advocates and those with memories of repressive governments both Communist and Nazi," writes Jake Tapper. "In 2013, the German magazine Der Spiegel, using information gleaned from files stolen and leaked by Edward Snowden, first reported that the NSA was intercepting German Chancellor Angela Merkel's cell phone communications."

Italian hackers...get hacked!
Over the weekend, an Italian surveillance and intrusion company known as "Hacking Team" got hacked, with a claimed 400 GB worth of proprietary data claimed to have been stolen from the company and posted online. CSO Online reports about the breach, which targeted a company pilloried over the years by privacy activists for allegedly selling hacking services to oppressive regimes. The leaked

data seems to add fuel to that fire. Check out the full story here.

Is the White House in compliance with cybersecurity rules?
-The White House's Executive Office of the President hasn't submitted reports detailing compliance with federal cybersecurity rules for the past three years, according to NextGov. "The apparent lack of annual reporting is even more striking considering the White House's unclassified computer networks were breached by hackers last fall, purportedly from Russia, leading to temporary outages as officials worked to suppress malicious activity," writes Jack Moore.

Pentagon to prep for cyber war
-The Pentagon expects to shift its planning away from countering extremist groups back to preparing for cyber war, largely in response to the growing menace of nation-state led cyberattacks, according to a newly released report. The report also hails the buildup of Cyber Mission Forces and the standup of the Joint Information Environment, a DoD-wide computer cloud, as crucial for preparing the military to fight future wars. Read more here.

DEA agent pleads guilty to Silk Road involvement
-In a development that reads like something out of a spy novel, a former DEA agent accused of using the Silk Road investigation to enrich himself pleaded guilty last week to extortion, money laundering and obstruction of justice. Wired.com reports that Carl Force, an undercover agent on the Silk Road investigation, admitted to using that position to steal bitcoins and act as a mole for drug dealers. "DEA special agent Carl Force and Secret Service special agent Shaun Bridges were arrested Monday and charged with wire fraud and money laundering," writes Wired's Andy Greenberg. "Bridges is accused of placing $800,000 of Silk Road bitcoins he obtained in a personal account on the Mt. Gox bitcoin exchange. But Bridges' charges pale in comparison with the accusations against the DEA's Force, who is additionally charged with theft of government property and conflict of interest in his investigation of the Silk Road. Force allegedly took hundreds of thousands of dollars worth of bitcoin payments from the Silk Road as part of his undercover investigation and transferred them to a personal account rather than confiscate them as government property."

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