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

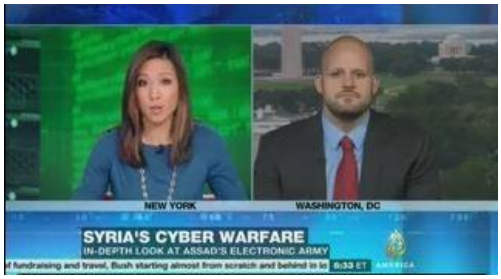
Follow CSPRI Director, Lance Hoffman: @lancehoffman1

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

June 29, 2015

Two (2) Cyber security events are scheduled in the Greater Washington Area in the next few weeks.

New interview



Aljazeera America interviewed CSPRI Senior Research Associate Trey Herr on June 17 about Syria's cyber warfare. See the video. Trey's comments begin at the02:45 minute mark.

Legislative Lowdown

-One of the pieces of technology legislation that has the most support from members of both sides of the aisle and both chambers of Congress can't seem to get a hearing, National Journal writes. The bill, The

Events

June 30
The Truth about Securing your System

July 8
Cyber Crime: Modernizing Our Legal Framework for the Information Age

Click here for detailed descriptions

Email Privacy Act, would update decades-old federal law by requiring law enforcement to obtain a search warrant before prying into the contents of private emails. Currently, authorities can get this information if it is stored in a cloud service online with just a subpoena if those records are at least 180 days old. "The bill, which would with more than 220 cosponsors in February, but has yet to earn a hearing or a vote in the House Judiciary Committee, where it boasts support from 23 of the panel's 39 members," reports Dustin Volz. "I think because it doesn't have the Edward Snowden sex appeal the NSA issues had, that it doesn't really register quite as significantly," the Journal quotes the bill's author as saying.

Cyber Security Policy News

Working around anti-virus software
- The National Security Agency and its British counterpart, Government Communications Headquarters, have worked to subvert anti-virus and other security software in order to track users and infiltrate networks, according to documents from NSA whistleblower Edward Snowden. The Intercept writes that the spy agencies have "have reverse engineered software products, sometimes under questionable legal authority, and monitored web and email traffic in order to discreetly thwart anti-virus software and obtain intelligence from companies about security software and users of such software. One security software maker repeatedly singled out in the documents is Moscow-based Kaspersky Lab, which has a holding registered in the U.K., claims more than 270,000 corporate clients, and says it protects more than 400 million people with its products." Read more here.

OPM update
-Federal investigators probing the massive data breach at the Office of Personnel Management (OPM) that exposed millions of records on government contractors and their families say they're not sure the extent of the breach at OPM because the agency and its contractors didn't have sufficient computer logs of the incident, NextGov reports.

Worse still, the attackers who broke into the OPM's systems appear to have had unfettered access to the agency's networks for at least a year, The Washington Post reports. "The considerable lag time between breach and discovery means that the adversary had more time to pull off a cyber-heist of consequence," Ellen Nakashima writes.

DoD thinking about changing cybersecurity regulations
-The Department of Defense is reportedly mulling changes that would discipline computer users on its network who run afoul of the agencies cybersecurity regulations. The DoD's chief information officer

"outlined his views on accountability during an address to an AFCEA conference on cyber defense, saying DoD needed to increase its overall focus on 'basic' defensive measures," according to a story in Federal News Radio. "He did not specify precisely what the new accountability measures could entail, but said they would be implemented by also making commanders responsible for the cyber behavior of the users under their charge. "

Cyber attack cancels 10 flights in Poland
-A Polish airline canceled 10 flights from an airport in Warsaw earlier this month after a cyber attack made it impossible for controllers and pilots to file flight plans. Computerworld writesthat a dozen or so other flights were delayed, and that the attack stranded some 1,400 passengers for more than five hours.

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