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 21, 2015

Four (4) events scheduled in the Greater Washington Area in the next few weeks.

Washington Post Cybersecurity Summit

The Washington Post in partnership with AT&T and The George Washington University Cyber Security and Policy Research Institute will host the Cybersecurity Summit on October 1, 2015 at The Washington Post.

Recent cyber attacks have wreaked havoc on companies and millions of people. Business leaders, lawmakers and security

Events

September 23
Meritalk: CSX Cyber Security Brainstorm

October 1
Cybersecurity Summit

October 1-2
Best Practices in Cyber Supply Chain Risk Management

October 5-6
ACFCS Cyber Financial Crime Summit

Click here for detailed descriptions

experts will discuss and debate the newest tools for cyber defense and policies to better protect companies, consumers and citizens.

Reserve your seat by clicking **here.**

Cyber Security Policy News

US and China: Cyberspace update
-The U.S. and China are trying to work out what could soon become the first arms control agreement for cyberspace, with each embracing a commitment by each country that it will not be the first to use cyberweapons to cripple the other's critical infrastructure during peacetime. "While such an agreement could address attacks on power stations, banking systems, cellphone networks and hospitals, it would not, at least in its first version, protect against most of the attacks that China has been accused of conducting in the United States, including the widespread poaching of intellectual property and the theft of millions of government employees' personal data," writes David E. Sanger. Read more here.

Government surveillance and cell phones
-The National Journal is running a primer on How the Government Surveils Cellphones, cataloging all the different ways the government can use your mobile devices to eavesdrop on citizens. "If law enforcement wants to surveil your cellphone, they have two ways to do it: They can do it through a phone company; or they can do it directly, using a device like a Stingray," writes Robinson Meyer in a story that first ran in The Atlantic.

2016 Presidential race websites fail privacy standards
-Most Web sites for the 2016 Presidential race fail basic privacy standards, according to a review by a security and privacy group. "Some websites failed due to nonexistent or inadequate privacy policy disclosures. Others flunked because they reserve the right to liberally share or sell their donors and site visitors' personally identifiable information ... with unaffiliated third parties that the candidates deem as like-minded organizations," according to a report released by the Online Trust Alliance. The information that can be shared includes addresses, phone numbers, employer information and even passport numbers, the report warns. The Hill hasmore coverage of the report.

Target Corp. under fire over data breach
-A federal judge last week cleared the way for banks to go after Target Corp. for damages related to the costs incurred by replacing 40 million credit and debit cards stolen by hackers in the 2013 breach. No doubt Exhibit A in the plaintiff's case will be a confidential internal penetration test conducted just days after the breach. Security journalist Brian Krebs

got a copy of that report, which looks at the weaknesses inside of Target's network that the attackers likely exploited. Citing the report, Krebs writes that the testers found "no controls limited their access to any system, including devices within stores such as point of sale (POS) registers and servers." In the report, the penetration testers hired by Target were able to communicate with registers in Target's many stores using a networked deli meat scale they'd compromised. Read more here.

US Cyber Challenge: Running more boot camps
-GovInfoSecurity carries a story that looks at the 6-year-oldU.S. Cyber Challenge, which operates four cybersecurity boot camps around the nation. "The one-week sessions are open to the top performers of the online competition," writes Eric Chabrow in a story that includes a video interview with Karen Evans, the program's national director. "With instructors from the SANS Institute and ISC2, campers are exposed to what it would be like to be a cybersecurity professional, Evans says, "in hopes that they would pursue an education and career path so we can fill the critical needs for the nation."

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