Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

The Weekly Newsletter of The George Washington University Cyber Security Policy and Research Institute

In This Issue

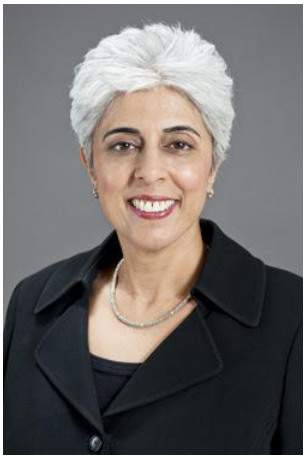
Quick Links

September 29, 2014

Ten (10) Cyber security Events are scheduled in the Greater Washington Area in the few weeks.

Announcements

Washington Post Cybersecurity Summit



The agency that brought you the Internet is now working on defending it. Hear Dr. Arati Prabhakar, director of the Defense Advanced Research Projects Agency, talk about unhackable drones, the next generation of encryption and the Cyber Grand Challenge that aims to build computer programs that can outsmart human hackers at The Washington Post's Cybersecurity Summit.

Events

Click here for descriptions of the upcoming events!

Click the Calendar to See Upcoming Events at a Glance!

Follow Us

Follow us on Twitter: @gwCSPRI

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

Follow CSPRI Research Scientist, Allan Friedman: @allanfriedman

WHEN
Wednesday, October 1, 2014
8:30 AM-12:00 PM
Doors open at 8:00 AM, Program begins at 8:30 AM.

WHERE
The Washington Post
1150 15th Street NW
Washington, DC 20071
Click here to reserve your seat, view event agenda and full list of speakers.

Legislative Lowdown

- The House and Senate are in recess.

-The prognosis for Congress getting anything done on cybersecurity this year is dim at best, according to an interview between GovInfoSecurity and Jim Lewis, director of the Strategic Technologies Program at the Center for Strategic and International Studies. Then again, maybe that's not such a bad thing. "Jim Lewis doesn't see Congress doing much legislating on cybersecurity, at least for the remainder of the current session that adjourns at year's end. And the nation won't be much worse off by the inaction," Eric Chabrow writes. In the wide-ranging interview, Lewis explains why nations such as China, Iran and Russia pose a greater cyberthreat to American and Western information technology than do terrorists.

Cyber Security Policy News

Shellshock
-Security experts around the globe are racing to devise and install security fixes for a newly-discovered, system software vulnerability that is being compared to the Heartbleed bug that was quashed earlier this year. Experts warn that attackers already are exploiting a critical security vulnerability present in countless networks and Web sites that rely on Unix and Linux operating systems. Experts say the flaw, dubbed "Shellshock," is so intertwined with the modern Internet that it could prove challenging to fix, and in the short run is likely to put millions of networks and countless consumer records at risk of compromise. "The bug is being compared to the recent Heartbleed vulnerability because of its ubiquity and sheer potential for causing havoc on Internet-connected systems - particularly Web sites,"writes Brian Krebs. "Worse yet, experts say the official patch for the security hole is incomplete and could still let attackers seize control over vulnerable systems."

Apple update

- Just days after Apple made headlines with news that its new mobile iOS operating system would prevent the government from accessing phone data even with a warrant, the company is getting a scolding from the FBI. According to the National Journal, Director James Comey told reporters he is "very concerned" that the new features could thwart critical police investigations. "What concerns me about this is companies marketing something expressly to allow people to place themselves beyond the law," Comey was quoted as saying.

Unhappy employees: a threat to data security?

-Disgruntled employees pose a serious risk to the security and integrity of corporate information, the FBI warned in a computer security bulletin released last week. "There has been an increase in computer network exploitation and disruption by disgruntled and/or former employees," the FBI wrote. Such employees have led to "several significant FBI investigations in which individuals used their access to destroy data, steal proprietary software, obtain customer information, purchase unauthorized goods and services using customer accounts, and gain a competitive edge at a new company," the bulletin continued.

Home Depot update

The FBI bulletin comes amid news that the former security architect at Home Depot is now serving a 4-year sentence for sabotaging his former employer's computer network after learning he was about to be terminated.

UK banks connect more with law enforcement

-Banks in the United Kingdom will be getting real-time information and warnings from law enforcement officials about threats to their customers' accounts, according to The Register. "Financial Crime Alerts Service (FCAS), which is being rolled out by banking industry association BBA, is designed to allow financial crime professionals to spot emerging problems and criminal trends based on data from 12 government and law enforcement agencies - including the UK's National Crime Agency (NCA)," writes John Leyden. "When it goes live, planned for early 2015, the BBA Financial Crime Alerts Service will include warnings on terrorist financing, money laundering, bribery and corruption, cybercrime and fraud. Subscribers will also get 'emergent, thematic and strategic reports' through the same online information hub."

Less transparency in the IT sector?

-The federal government has taken a great deal of heat from the public over the secrecy surrounding

its various domestic spying programs, but technology companies aren't exactly tripping over themselves to be transparent about their financial support of federal lawmakers, according to a new report. The analysis, by the Center for Political Accountability and the University of Pennsylvania's Zicklin Center for Business Ethics, found that the information technology sector ranked near the bottom of industries it reviewed.

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
304 Staughton Hall
707 22nd St., NW
Washington DC, DC 20052