GW CSPRI Newsletter

November 12, 2012

From the **Cyber Security Policy and Research Institute** of **The George Washington University**, www.cspri.seas.gwu.edu.

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.

Faculty and student readers of this newsletter with new and important cyber security research to report (especially new papers or results by GW faculty and students) are encouraged to send notifications of this to cspriaa@gwu.edu. A short (up to three sentences) description of why you think the research is important is required.

Contents

Events

Legislative Lowdown

Cyber Security Policy News

Events

-Nov. 12, 5:30 p.m. - 8:30 p.m., **NoVa Hackers Assocication Meetup** - This informal group of security professionals from around the NoVa/DC area coordinates one or two monthly events – an evening meetup with presentations on the second Monday of the month and various lunch or bar meetups. 11091 Sunset Hills Road, Reston, VA. More information.

-Nov. 13, 2:00 p.m. - 4:00 p.m., **Privacy Multistakeholder Process: Mobile Application Transparency** - The Department of Commerce's National Telecommunications and Information Administration will hold another in a series of meetings regarding consumer data privacy in the context of mobile applications. This event will be webcast. 1401 Constitution Ave., NW. More information.

-Nov. 14, 10:00 AM - 12:00 noon, **Should the UN Control the Internet?** - The American Enterprise Institute will host a panel discussion, ahead of the meeting of the World Conference on International Telecommunications in early December. The speakers will be Terry Kramer, Ambassador, head of the US delegation to the WCIT; Fiona Alexander, NTIA; Leonard Cali, AT&T; David Gross, Wiley Rein; Ross LaJeunesse, Google; Robert McDowell, FCC Commissioner; and Jeffrey Eisenach, American Enterprise Institute. 12th floor, 1150 17th St., NW. More information.

-Nov. 14, **ISACA CM Meetup: Security Issues From Your Wired to Wireless Network** - The ISACA – Central Maryland (CM) chapter is based in Baltimore, MD. Chapter meetings are usually held nine times per year. The Conference Center at the Maritime Institute, 692 Maritime Boulevard, Linthicum, MD. More information.

-Nov. 14-15, **Industrial & National Security Compliance: Strategic Insights on Managing DSS Vulnerability Assessments, Classified Information, FOCI Mitigation and Cyber Security Risks** - Hear insights from leading legal, compliance, security and trade executives from the most prestigious firms in the country. Hear experiences of others and see how other companies are dealing with counterintelligence threat assessments, cybersecurity risk management, FOCI mitigation, and CFIUS review roadblocks as mergers and acquisitions continue to make a comeback. Hilton Arlington, 950 North Stafford Street Arlington, Va. More information.

-Nov. 15, 7:30 a.m. - 4:30 p.m., **FedCyber.com Cyber Security Summit** - Talks at this year's conference will focus on three key areas: threat intelligence, adversary characterization, and information sharing; cyber workforce challenges; and emerging technologies that will change the cyber security landscape. Ronald Reagan Building, 1300 Pennsylvania Ave. NW. More information.

-Nov. 15, 12 noon - 1:00 p.m., **Medical Device Cybersecurity: The First 164 Years** - Prof. Kevin Fu of the University of Massachusetts-Amherst will host this free event. This talk will provide a glimpse into the risks, benefits, and regulatory issues for medical device cybersecurity and innovation of trustworthy medical device software. The session will be webcast as well. To attend virtually, please register here. After your registration is accepted, you will get an email with a URL to join the meeting. National Science Foundation, Stafford I Building, Room 110, in Ballston, Va.

-Nov. 15, 1:00 p.m., **Mitigating e-Fraud Security Risks for 2013 and Beyond** - Join Michael Osterman and Michael Knight, VP Solution Services of TrustSphere for a Webinar on what to expect from organized eFraud over the next year, and how to counter those threats. More information.

Legislative Lowdown

-Senate Majority Leader Harry Reid (D-Nev.) may take another crack at passing cybersecurity legislation next week although Republicans and Democrats still haven't reached a compromise on the matter, The Hill reports. Reid is aiming to bring the Cybersecurity Act of 2012 to the floor at the end of this week. The bill's prospects look dim, however, as it appears the bill still lacks enough Republican support to clear the upper chamber. Observers expect the bill to fail just as it did in August, when Senate Republicans blocked a motion to move the measure forward after arguing that it would saddle industry with new burdensome regulations.

-Mobile industry policy experts on Thursday said cybersecurity, privacy, and spectrum would be among the top issues facing the mobile industry in 2013, the National Journal reports. Earlier this year, the administration unveiled a proposal to boost online consumer privacy through a consumer "Privacy Bill of Rights." While the White House called on Congress to implement this proposal through legislation, it also is pushing for industry to implement some of the principles through voluntary industry codes of conduct. The first industry stakeholder effort aimed at developing these codes of conduct is focused on increasing transparency in what data is collected by mobile applications.

That focus on privacy is almost assured, given lawmakers' apparent renewed interest in what data brokers are doing with consumer information. National Journal's Juliana Gruenwald writes that a bipartisan group of House members said on Thursday they are not satisfied with responses they got from nine data brokers, saying the industry needs to be more open about how it uses personal information collected about consumers. Reps. Edward Markey, D-Mass., and Joe Barton, R-Texas, co-chairmen of the Congressional Bipartisan Privacy Caucus, and five other lawmakers wrote nine data brokers last summer seeking more information about where they collect data, what type of data is collected, who buys the data, and how it is used. The lawmakers said in a statement that only one company, Acxiom, described itself as a data broker. In its response to the lawmakers, Equifax, which is more well known as one of the three national credit reporting agencies, rejected the data broker label and instead said it offers "marketing services," which it noted only make up 1 percent of its business.

Cyber Security Policy News

-Despite a Securities and Exchange Commission (SEC) rule requiring companies to report any material losses from cyber attacks, many are keeping investors in the dark long after significant break-ins, Bloomberg found in a lengthy investigation. The publication ran a story last week showing how Coca Cola hid the evidence of an extended, targeted cyber attack that resulted in the loss of proprietary data at the hands of Chinese hackers. According to Bloomberg, FBI officials quietly approached executives at Coca-Cola Co. on March 15, 2009, with some startling news. Hackers had broken into the company’s computer systems and were pilfering sensitive

files about its attempted $2.4 billion acquisition of China Huiyuan Juice Group, according to three people familiar with the situation and an internal company document detailing the cyber intrusion. The Huiyuan deal, which collapsed three days later, would have been the largest foreign takeover of a Chinese company at the time.

-South Carolina lawmakers are among those being named in a class action lawsuit being filed in the wake of a breach in the state that exposed as many as 657,000 S.C. businesses and the Social Security records of up to 3.6 million state residents. The class action lawsuit filed last week says Gov. Nikki Haley and other state officials failed to protect millions of South Carolina residents victimized by a recent security breach. In a news release, John Hawkins -- a former South Carolina state senator -- said Haley and officials with the state Department of Revenue failed to adequately protect those victims. Hawkins said state officials violated state law that requires "prompt disclosure" of such breaches. "This hacking amounts to a 'Cyber Hurricane' and it's a Category 5," said Hawkins in the news release.

-A record number of tech products used by the U.S. military and dozens of other federal agencies are fake, exposing personnel to a myriad of national security risks, from dud missiles to short-circuiting airplane parts to cyberespionage, according to CNN Money. Despite laws designed to crack down on counterfeiters, suppliers labeled by the U.S. government as "high risk" are increasing their sales to federal agencies. Their presence in government's supply chain soared 63% over the past decade, according to a new study released by IHS, a supply chain management consultancy. Suppliers with the high-risk branding are known to engage in counterfeiting, wire fraud, product tampering and a laundry list of other illicit and illegal behaviors. Last year, 9,539 banned businesses were found to have sold technology the government. Roughly 10% of those incidents involved counterfeit parts or equipment.

-A federal judge is ordering the Justice Department to disclose more information about its so-called “Going Dark” program, an initiative to extend its ability to wiretap virtually all forms of electronic communications, Wired.com writes. The ruling by U.S. District Judge Richard Seeborg of San Francisco concerns the Communications Assistance for Law Enforcement Act, or CALEA. Passed in 1994, the law initially ordered phone companies to make their systems conform to a wiretap standard for real-time surveillance. The Federal Communications Commission extended CALEA in 2005 to apply to broadband providers like ISPs and colleges, but services like Google Talk, Skype or Facebook and encrypted enterprise Blackberry communications are not covered. The FBI has long clamored that these other communication services would become havens for criminals and that the feds would be left unable to observe them, even though documents acquired by Wired shows that the FBI’s wiretapping system is robust and advanced.

-The United States has the technical capability to secure its networks from cyber threats, but until Congress takes action on cybersecurity legislation, security improvements are stopped in their tracks, the head of the National Security Agency said last week. Gen. Keith Alexander, the director of NSA and the commander of U.S. Cyber Command, said he thinks the biggest barrier to improving the nation's overall cyber posture boils down to a basic lack of education in the

nation, both about how networks operate and about the scope of the threat. Speaking to a government and IT security industry audience Wednesday, Alexander showed frustration about the slow pace toward updating the nation's cyber laws and said failing to prepare ahead of time for cyber attacks would lead to "bad decisions" should U.S. critical infrastructure come under attack from actors such as those who targeted Aramco, Saudi Arabia's state-owned oil company, earlier this year.

At the same time, The Consortium for Cybersecurity Action, a newly-formed international group of government agencies and private organizations from around the world, last week released an updated baseline of the 20 most important cyber controls, Federal News Radio writes. The group said it wants to become a resource to help agencies implement those security checks. The idea got positive reviews from Tony Sager, a director with the SANS Institute and a former chief operating officer of the National Security Agency's Information Assurance Directorate, who said many of these 20 controls are basic, but important. Sager said this update comes as the Homeland Security Department is using the guidelines as part of its effort to implement continuous monitoring. DHS also is preparing a solicitation to buy continuous monitoring-as-a-service and tools that includes some of these security steps.

The Cyber Security Policy and Research Institute (CSPRI) is a center for GW and the Washington area to promote technical research and policy analysis of problems that have a significant computer security and information assurance component. More information is available at our website, http://www.cspri.seas.gwu.edu.