GW CSPRI Newsletter

March 4, 2014

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 1

Legislative Lowdown 2

Cyber Security Policy News 2

Events

-Mar. 4, **Cybersecurity Summit 2014** - Attendees will have an opportunity to hear what challenges Department of Defense and federal cyber leaders are facing today; engage in breakout sessions on critical topics; network with cyber professionals and discuss new ideas and solutions; and hear where agencies are headed and where the budgets are in 2014. Capital Hilton, 1001 16th St. NW. More information.

-Mar. 5, 10:00 a.m., **Data Security: Examining Efforts to Protect Americans' Financial Information** - Speakers will include William Noonan, deputy special agent in charge, Criminal Investigation Division, Cyber Operations, United States Secret Service; Troy Leach, chief technology officer, PCI Security Standards Council; Greg Garcia, advisor, Financial Services Information Sharing and Analysis Center; David Fortney, senior vice president, Product Management and Development, The Clearing House Payments Company; Edmund Mierzwinski, consumer program director, U.S. PIRG. Rayburn House Office Bldg., Room 2128. More information.

-Mar. 5-7, **IAPP Global Privacy Summit 2014** - Washington Marriott Wardman Park, 2660 Woodley Rd. NW More information.

-Mar. 6, 9:30 a.m., **Can Technology Protect Americans from International Cybercriminals?** - The Subcommittee on Oversight and Subcommittee on Research and Technology will hold a joint hearing. Witnesses will include Charles H. Romine, director, Information Technology Laboratory, National Institute of Standards and Technology; Bob Russo, general manager, Payment Card Industry Security Standards Council, LLC; Randy Vanderhoof, executive director, Smart Card Alliance; Justin Brookman, director, Consumer Privacy, Center for Democracy & Technology; Steven Chabinsky, senior vice president of legal Affairs, CrowdStrike, Inc. and former deputy assistant director, Federal Bureau of Investigation – Cyber Division. Rayburn House Office Bldg., Room 2318. More information.

-Mar. 7, **LEC Research Roundtable on the Future of Privacy & Data Security Regulation** - George Mason University School of Law3301 Fairfax Drive, Arlington, Va. 22201. More information.

-Mar. 10-12, **2014 AFCEA Homeland Security Conference** - This conference offers an opportunity for attendees to engage with key government and industry leaders on critical security matters. Conference tracks will address big data analytics; continuous diagnostics monitoring; information sharing; and professionalization of cyber security. Ronald Reagan Building and International Trade Center - Atrium Hall and Ballroom, 1300 Pennsylvania Ave, NW More information.

Legislative Lowdown

-Legislation in the House that would end the warrantless searches of email records is gaining steam. According to The Hill, "privacy advocates had grown frustrated in recent months as Senate legislation that would curtail the email powers of law enforcement was thrown off track amid revelations about National Security Agency surveillance. But they are increasingly optimistic that an update to the 1986 Electronic Communications Privacy Act (ECPA) — which allows law enforcement agencies to obtain things like emails without a warrant if they have been stored electronically for more than 180 days — could see action in the House. There's a lot of growing support for that bill," The Hill quotes Mark Stanley of the Center for Democracy and Technology. "A lot of members of Congress see this as a common sense thing."

Cyber Security Policy News

-The president of China said last week he was presiding over a new working group on cybersecurity and information security, according to The New York Times. The Times reports that President Xi Jinping would join several leaders to "help draft national strategies and develop major policies in a field that might include protecting national secrets and developing digital defenses, among other goals," and that the move was "a sign that the Communist Party views the issue as one of the country's most pressing strategic concerns."

In South Korea, the government is aiming to develop cyber-attack tools in an attempt to damage North Korean nuclear facilities, the BBC reports. "The country's defense ministry wants to

develop weapons similar to Stuxnet, the software designed to attack Iranian nuclear enrichment plants. The South Korean military will carry out missions using the software, the defense ministry said. In 2006, North Korea claimed it had successfully tested a nuclear weapon, spreading alarm through the region. Intensive diplomatic efforts to try to rein in North Korea's nuclear ambitions continue."

Sears may be the latest retail giant to investigate compromises of its store payment systems, according to several media reports last week. But as Brian Krebs of KrebsOnSecurity.com reports, the rumor mill about which major retailer will announce a breach next has been running at full steam in recent weeks, putting many retailers in an awkward position. Krebs quotes Bryan Sartin of Verizon Enterprise Solutions as noting that the main mechanism that many banks have for diagnosing the source of card breaches -- a fraud tracking tool known as "common point of compromise" -- works very well, except in the wake of giant breaches like the one announced last year at Target. "The problem of false positives often come from small institutions that may not have a broader perspective on how far a breach like Target can overlap with purchasing patterns at similar retailers," Krebs writes. "And that can lead to a costly and frustrating situation for many retailers, particularly if enough banks report the errant finding to Visa, MasterCard and other card associations. At that point, the card brands typically secure guarantees that the identified merchant hire outside investigators to search for signs of a breach."

Meanwhile, Target has hired a pair of lobbyists to push lawmakers on data breach issues, weeks after a hack exposed the personal and financial data of as many as 110 million of the store's shoppers, reports The Hill. "Both lobbyists are former staffers on Capitol Hill. William Nordwind, a partner at Venable, used to work for Rep. Fred Upton (R-Mich.), the chairman of the House Energy and Commerce Committee," The Hill's Julian Hattem writes. "He also spent time as a counsel on the panel's telecommunications subcommittee and as a staffer for former Rep. Deborah Pryce (R-Ohio). Robert Smith, a senior legislative advisor with the law firm, spent time in the offices of former Reps. Wes Watkins (R-Okla.) and Joel Hefley (R-Colo.)."

-The Federal Trade Commission announced last week that for the 14th consecutive year, identity theft topped the list of complaints the agency receives from consumers. In a statement and report, the FTC said that of the more than 2 million consumer complaints received, "identity theft leads the field, with 14 percent of total complaints filed. Thirty percent of those were tax- or wage-related, which continues to be the largest category within identity theft complaints. Coming in at a close second: debt collection, with 10 percent. Completing the trifecta: banks and lenders, with 7 percent."

-The White House has issued guidance to help school systems and teachers protect their students' information online. The document, released last week by the Department of Education, encourages school districts to use more scrutiny to protect student privacy when using online educational services, and clarifies which information is covered under federal law and what the government requires of schools. According to The Associated Press, "a patchwork of laws spells out how students' data can be used, but the laws can be difficult for districts to interpret. Some privacy advocates say laws haven't kept up with evolving technology, and there's been a flurry of activity at the state and federal level to address the issue."

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.