GW CSPRI Newsletter

May 12, 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

-May 13-14, **The Future of Privacy and Data Security Regulation** - The George Mason University Law School's Law and Economics Center will host a conference. GMU law school, 3301 Fairfax Drive, Arlington, VA. More information.

-May 13-14, **Cyber Security for National Defense Symposium** - This conference is designed as an educational and training "Town Hall" forum, where thought leaders and key policymakers across military and civilian organizations can come together for actionable discussions and debate. The symposium will focus on increasing the security and resiliency of the Nation’s critical networks, operating freely in the Cyber Domain, and the protection of infrastructure in support of national defense and homeland security. Defense Strategies Institute, 20 F. St. NW. More information.

-May 14, 8:00 a.m., **Disrupting Defense: Dynamic Security in an Age of New Technologies** - Join the Atlantic Council's Brent Scowcroft Center on International Security on May 14, when they will convene experts to discuss how the United States and its allies can manage the security-related challenges and possibilities of disruptive technologies. 1030 15th Street, 12th Floor (West Tower). More information.

-May 15, 9:30 a.m., **Online Advertising and Hidden Hazards to Consumer Security and Data Privacy** - The Permanent Subcommittee on Investigations has scheduled a hearing. The Subcommittee will be examining consumer security and data privacy in the online advertising industry, an investigation led by Senator McCain. Specifically, the Subcommittee is investigating data collection processes and security vulnerabilities that have inflicted significant costs on Internet users and American businesses. Witnesses will include representatives of the online advertising industry and an online self-regulatory organization, an online advertising expert, as well as a representative from the Federal Trade Commission. A witness list will be available Monday, May 12, 2014. Dirksen Senate Office Bldg., Room 342. More information.

-May 15, 10:30 a.m. -11:30 a.m., **Webcast Q&A: Board Considerations As To Cybersecurity Risk Management** - This high-level discussion & debate will seek to go well beyond merely reciting mandate specifics to address in a highly interactive forum what might Board Members do going forward to better control potential regulatory/reputational risk exposure, as well as their financial firm’s global market competitiveness. To attend this webcast "live" or to receive a web link to the recording, please email the head of CBG (JPWilson@GCCG.biz).

-May 21, 10:00 a.m., **Assessing Persistent and Emerging Cyber Threats to the U.S. Homeland** - The Committee on Homeland Security’s Subcommittee on Counterterrorism and Intelligence and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will hold a joint hearing that was rescheduled from May 8. Cannon House Office Bldg., Room 311. More information.

-May 21-22, **2nd Annual Cybersecurity Law Institute** - This year’s Institute seeks to help lawyers from companies, private practice, and state and federal government deal more effectively with the growing number of cybersecurity risks. Currently, besides a few industry-specific areas, there are no federal regulations governing breach notification, and state laws have varying degrees of rigidity regarding breaches. This program brings together regulators, enforcers, and in-house and outside counsel to have productive dialogue about these challenges. Georgetown University Law Center, Continuing Legal Education, 600 New Jersey Avenue NW. More information.

-May 22, 8:30 a.m. - 5:00 p.m., **Cyber Montgomery** - The CyberMontgomery Forum was developed jointly by The Montgomery County Department of Economic Development and the Federal Business Council in conjunction with leaders from federal and local government agencies, industry and academia. Cybersecurity will be a major growth engine in the region for many years to come. With solid federal government, industry and academic assets already in place in the region, there is still a need to bring them together so that they can coalesce and elevate the cyber ecosystem to a level of national prominence. CyberMontgomery Forum events will provide clear direction on finding business opportunities, contracting, forecasted demand areas, workforce development, recruiting & staffing, legal responsibilities for businesses, updates on technologies being developed in MoCo and summary updates regarding our NCCoE neighbors, federal civilian agencies and commercial sector leaders. Universities at Shady Grove (USG), 9630 Gudelsky Drive, Rockville, MD 20850. More information.

-May 22, 8:30 a.m. - 6:00 p.m., **Business Insurance Cyber Risk Summit** - This is a leadership conference created to guide corporate executives, risk managers, legislators and policymakers, regulators, law firms, consultants, technology executives, and insurance industry executives as they define standards—and a common governance framework—for shared responsibility, protection and recovery from the rapidly accelerating exposure to and threat from cyber-crime and other cyber-related attacks. W Washington D.C. 515 15th Street N.W. More information.

Legislative Lowdown

-A House panel last week approved a measure to reform the NSA's surveillance activities, including curbs that would end the spy agency's bulk collection of Americans' phone records, The Washington Post reports. Nearly a year after former NSA contractor Edward Snowden disclosed the existence of this practice, the House Judiciary Committee voted unanimously to rein in the NSA with the USA FREEDOM Act, a measure that places new requirements on the government when it comes to gathering, targeting and searching telephone metadata for intelligence purposes. "In addition to prohibiting the NSA from engaging in what the bill's sponsors have called 'dragnet surveillance,' the bill would also require authorities to get permission from the secret Foreign Intelligence Surveillance Court on a case-by-case basis," The Post's Brian Fung writes. "It would establish a panel of privacy experts and other officials to serve as a public advocate at the court. And it would also give businesses more latitude to tell the public about requests it receives from the government for user data."

-A House committee voted to delay the White House's plan to relinquish authority over the Internet's address system. Voting along party lines, the House Energy and Commerce Committee passed the DOTCOM Act, which requires that the Government Accountability Office study the issue before the Commerce Department could give up its contractual authority over the Internet Corporation for Assigned Names and Numbers—the nonprofit group that manages the technical procedures that allow computers around the world to connect to websites. The transfer of authority over ICANN to the "global Internet community" is scheduled to take place next year, but as Brendan Sasso writes for National Journal, "Republicans fear the administration's plan could allow Russia, China, or other authoritarian regimes to seize new powers over the Internet and even censor websites."

Cyber Security Policy News

-Apple last week released an extensive document describing what data the company can provide to law enforcement and the processes for requesting that data, Ars Technica reports. The move comes as the U.S. Supreme Court considers whether police should be able to search and use data stored on smart phones of arrested suspects. Andrew

Cunningham breaks it down: "The short version is that essentially anything you've backed up to or stored on iCloud is available for Apple to fork over to law enforcement, including connection logs and IP addresses you've used. Apple has access to 60 days of iCloud mail logs that 'include records of incoming and outgoing communications such as time, date, sender e-mail addresses, and recipient e-mail addresses'; any e-mail messages that the user has not deleted; and any other information that can be backed up to iCloud. As of this writing, this list includes contacts, calendars, browser bookmarks, Photo Stream photos, anything that uses the 'documents and data' feature (which can include not just word processors but also photo and video apps, games, and data from other applications), and full device backups. Subscriber information requires a 'subpoena or greater legal process,' e-mail logs require a court order or search warrant, and e-mail or other iCloud content requires a search warrant. Any iCloud information that the user deletes cannot be accessed."

-A new report (PDF) from the White House's Office of Management and Budget finds that federal agencies and departments are showing progress in implementing solutions designed to fight increasingly sophisticated cyber threats. GovInfoSecurity.com analyzed the report, and found that in 2012, "government agencies, on average, met 73 percent of the [federal information security] requirements. That percentage rose to 81 percent last year, with significant improvements in adoption of automated configuration management, remote access and e-mail encryption. Compliance with cross-agency performance goal strategies saw similar improvements, with average agency compliance rising from 77 percent in 2012 to 81 percent in 2013. CAP goals include trusted internet connections, continuous monitoring and strong authentication."

-The Consumer Financial Protection Bureau (CFPB) is urging banks and other financial institutions to publish privacy disclosures online, in a bid to ensure that information about their data-sharing activities is more accessible to consumers. As The Hill writes, the CFPB announced last week that it is considering a new rule intended to limit banks' data-sharing activities and improve transparency, a move it claimed would save the industry millions of dollars each year. "Currently, banks are required to mail privacy disclosures to their customers once a year," writes Tim Devaney. "But the new rules would instead allow these disclosures to be posted online, under certain conditions." Read more here.

-A data spill that stemmed from a doctor's attempt to reconfigure a server cost New York Presbyterian Hospital and Columbia University Medical Center $4.8 million to settle with the U.S. Department of Health and Human Services, ComputerWorld reports. According to Jaikumar Vijayan, the $3.3 million settlement with New York Presbyterian is the largest ever obtained by the HHS for a violation of HIPAA security rules. "The hospitals and HHS announced the voluntary settlement, which ends an inquiry into the incident, on Wednesday," Vijayan writes. "New York Presbyterian will pay $3.3 million, while Columbia will pay $1.5 million to settle the complaint."

Not all government enforcement is as costly. Last week, app maker SnapChat settled charges with the Federal Trade Commission that it deceived customers about privacy and security claims, but as CNN reports, the Los Angeles-based startup is essentially getting a slap on the wrist. "The heart of the issue is Snapchat's assurance that customers' messages were safe and private. Snapchat's whole business was built on that promise," CNN's Jose Pagliery writes. "For instance, Snapchat photos have a self-destruct timer. But recipients could get around the auto-destruct by saving an image of what was on the screen. It has to allow independent privacy auditors to inspect the company for the next 20 years, and it was forced to promise it will be more forthright with customers. That's about it."

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.