GW CSPRI Newsletter

May 19, 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

Announcements

"Chinese military unit charged with cyber-espionage against U.S. firms": Click here to read.

Events

-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, 6:00 p.m. - 9:00 p.m., **NovaInfosec Meetup, West** - A casual meetup of information security professionals and enthusiasts in Northern Virginia. Velocity Five, 19286 Promenade Dr., Leesburg, Va, 20176. 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. 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.

-May 22, 9:00 a.m. - 4:35 p.m., **IT Professional Conference: Challenges in Information Systems** - This conference, organized by IEEE IT Professional magazine, seeks to bring together IT professionals and managers from industry, government, and academia to examine the new challenges facing Information Systems, and to explore how they can be successfully addressed. What are today's biggest challenges getting the most value from investments in information technology, while delivering successful projects and reliable information systems and infrastructure? How do we prevent critical systems from being compromised while keeping pace with advances in technology? What are the approaches that successful organizations are applying to deal with these challenges now? What is on the horizon that technology and business leaders need to anticipate? How can we make our information systems and applications better -- smarter, resilient, reliable, and secure? Green Auditorium, NIST 100 Bureau Drive, Gaithersburg, MD 20899. More information.

-May 22, 2:00 p.m. - 3:30 p.m., **Tackling Emerging National Security Threats Through Law Enforcement** - On May 22, Governance Studies at Brookings will host John Carlin, Assistant Attorney General for National Security at the U.S. Department of Justice, for a discussion of how the Department is adapting and responding to the changing threat picture. Mr. Carlin will address, in particular, the role of the National Security Division in tackling emergent threats such as those in cyber space. This event will also be Webcast. Brookings Institution, Saul Room/Zilkha Lounge, 1775 Massachusetts Av., NW. More information.

-May 29, 7:00 p.m. - 10:00 p.m., **CharmSec Meetup** - An informal, all-ages, citysec-style meetup of information security professionals in Baltimore. Heavy Seas Alehouse, 1300 Bank St., Baltimore, Md, 21231. More information.

Legislative Lowdown

-Technology groups are unhappy with a bill to reform the NSA that is coursing through the House of Representatives. "Passing the USA Freedom Act would be an historic event in favor of privacy, but the bill certainly does not address all the significant human rights issues raised by over-broad national security surveillance," wrote Harley Geiger, senior counsel with the Center for Democracy and Technology, in a blog post. According to The Hill, the groups want reforms "to limit 'backdoor' searches on Americans, allow private companies to disclose more information about the requests for data they receive from the government and appoint a special advocate to the Foreign Intelligence Surveillance Court, instead of a panel of advisors. The letter was signed by major Web companies like Facebook, Google and Apple, which have banded together under the Reform Government Surveillance coalition, as well as privacy and civil rights advocates like the Center for Democracy and Technology, the American Civil Liberties Union and FreedomWorks."

Cyber Security Policy News

-The Justice Department is expected to announce today that it will file charges against several hackers in China's People's Liberation Army (PLA), accusing them of stealing trade secrets from American companies. The move, says The New York Times, would mark the first time the United States has charged state actors with economic espionage. In a separate case, the department will announce charges against several people who used a hacking software called Blackshades. The software allows hackers to remotely control a computer, the Times reports.

-The FBI wants to make it easier to hack suspects' computers remotely, The Washington Post reports. "The Justice Department is seeking a change in criminal rules that would make it easier for the FBI to obtain warrants to hack into suspects’ computers for evidence when the computer’s physical location is unknown — a problem that officials say is increasing as more and more crime is conducted online with tools to conceal identity," writes Ellen Nakashima. "But the proposal, which was posted for public comment on a U.S. court Web site Friday, is raising concerns among privacy advocates who see it as expanding the power of federal agents to insert malware on computers, which they say could weaken overall Internet security. The proposed change would also make it easier for agents to use one warrant to obtain evidence on possibly hundreds or thousands of computers spread across the country when the machines have been secretly commandeered into “botnets” by criminals to conduct cyberattacks."

-In the latest sign that cybersecurity is big business in Washington, last week saw the release of a reporting indicating that the number of companies, associations and other groups lobbying on data and cybersecurity issues has nearly tripled since 2008, according to a review by Capitol Metrics, a lobbying analytics firm. The number of lobby firms advocating on behalf of clients on data and cybersecurity issues also tripled in the same period. Writing about the report, The Washington Post reports that "between 2008 and 2012, the number of companies, trade associations and other groups lobbying on data or cybersecurity matters climbed steadily from 108 to 321, and dipped slightly in 2013 to 314. Those figures reflect lobbying activity by companies' in-house lobbyists who listed 'data security,' 'cybersecurity' or 'cyber security' on lobbying disclosure forms."

For its part, the General Services Administration definitely believes cybersecurity has a strong future in Washington. So much so that it's planning to build a 630,000 square foot campus to house cyber experts from the Department of Homeland Security, FBI and other agencies. "With the federal government facing an increasing threat from cyber attacks, the campus would be designed so federal agencies and private sector companies can better share information about those threats and how to counter them," writes Daniel J. Sernovitz, for the Washington Business Journal. "The agency, which oversees the federal government's real estate needs, outlined its vision for the campus in a prospectus posted recently to its website."

-From the "need-a-bigger-hard-drive department" comes a strange story of a spy plane whose data-hoovering capabilities crashed an air traffic control tower computer, delaying flights across the U.S. in April. According to Reuters, "a common design problem in the U.S. air traffic control system made it possible for a U-2 spy plane to spark a computer glitch that recently grounded or delayed hundreds of Los Angeles area flights, according to an inside account and security experts. In theory, the same vulnerability could have been used by an attacker in a deliberate shut-down, the experts said, though two people familiar with the incident said it would be difficult to replicate the exact conditions." Reuters writes that the glitch blacked out a large chunk of the southwestern Unted States.

-In the wake of costly data breaches at big retail names like Target, Neiman Marcus and Michaels, a group of major U.S. retailers have formed a group for sharing cyber threat information. The Retail Cyber Intelligence Sharing Center (R-CISC) includings J.C. Penney, Gap, Lowe's, Nike, Safeway, Target, Walgreen, American Eagle Outfitters, and VF Corp., which owns more than a dozen brands. CSO Magazine notes that "the centerpiece of the center's strategy for bolstering security is the Retail Information Sharing and Analysis Center (Retail-ISAC), which will be responsible for 'identifying real-time threats and sharing actionable intelligence to mitigate the risk of cyberattacks.' How all that will be done is not clear."

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.