Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

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

Quick Links

About CSPRI

Contact Us

Newsletter Archive

Blog: The CSPRI Byte

New!

Read more about CSPRI's education, research, and service projects with our new, interactive project wheel.

Click here.

April 20, 2015

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

Legislative Lowdown

-A digital surveillance bill expected to be introduced this week in the House would force the National Security Agency to obtain text and call records by working directly through the major phone providers. "The bill, known as the USA Freedom Act, would effectively end the NSA's bulk collection of U.S. phone metadata-the numbers, time stamps, and duration of a call but not its actual content-by instead relying on phone companies to retain that data,"writes Dustin Volz at The National Journal. "The program is the first and one of the most controversial spying programs exposed by the Edward Snowden leaks that began nearly two years ago." There appears to be a latent sense of urgency among lawmakers for action on the measure, since the bill's introduction arrives as the window of opportunity for reforming the nation's surveillance activities is rapidly closing, Volz observed. "Core provisions of the post-9/11 Patriot Act are due to sunset on June 1, including the controversial Section 215, which the NSA uses to authorize its dragnet surveillance of Americans' call data. The Freedom Act would reauthorize these authorities, preserving expiring capabilities the intelligence

Events

See Upcoming Events at a Glance

Click here for detailed descriptions

Follow Us

Follow us on Twitter: @gwCSPRI

Follow CSPRI Director, Lance Hoffman: @lancehoffman1

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

community has said are vital to national security while ushering in more strident privacy protections and transparency requirements."

-The House Committee on Rules will meet on **Tuesday, April 21, 2015** at **5:00 PM** in H-313 The Capitol on the following measures: H.R. 1560-Protecting Cyber Networks Act and H.R. 1731-National Cybersecurity Protection Advancement Act of 2015.

Cyber Security Policy News

RSA Security Conference
-The RSA Security Conference, the largest security industry gathering in the world, kicks off in San Francisco today, where more than 20,000 people will meet to share information about the latest in techniques and approaches to fighting cyber fraud. Judging from the tenor of talks slated throughout this week at RSA, a big focus this year seems to be "threat intelligence" and beefing up authentication and authorization beyond merely identifying customers and consumers via static identifiers as an unprecedented glut of stolen data is flooding the underground cybercrime markets.

WiFi security on planes
Many of the security executives not already in San Francisco will be flying there today for RSA, and surely some of them are grateful if their plane does not have WiFi on board. Having a few hours to unplug from the office is nice, but report out last week from the Government Accountability Office (GAO) offers another reason for relief at the respite: hackers using the plane's bundled WiFi service to manipulate the instrumentation and other technology on airplanes. Wired.com reports: "Seven years after the Federal Aviation Administration first warned Boeing that its new Dreamliner aircraft had a WiFi design that made it vulnerable to hacking, a new government report suggests that passenger jets might still be vulnerable. But according to Forbes, there's no need to prep your parachute: The GAO's report, Forbes alleges, "was put together by people who didn't understand how modern aircraft actually work." Alan Paller, director of research at the SANS Institute, remarked in SANS's email newsletter that he would "normally reject that type of argument as light-weight whining, but in GAO's case I would be making an error. GAO staffers have demonstrated repeatedly that they do not understand how attacks and networks and operating systems work - at the deep technical level," Paller wrote. "That means their reports have been forcing government agencies to spend money in precisely the wrong ways - so much so that a close analysis will show that GAO is culpable in enabling the deep and pervasive cyber

penetration that has occurred across many elements of the federal government. GAO staffers blame OMB's regulations for their errors when they are called to account. Isn't it time for GAO leadership to take a hard look at the damage caused by its findings and the people they have making those findings?"

Sony leak: update

-Likely much to the chagrin of Hollywood executives and the entertainment industry, whistleblower Web site WikiLeaks has made tens of thousands of leaked Sony documents easily searchable on its website. As Mario Trujillo reports for The Hill, the anti-secrecy group said its searchable archives contain more than 30,000 documents and 173,00 emails, which were leaked last year as part of a massive hack of Sony Pictures Entertainment that the United States blamed on North Korea.

China: new technology policy for banks

-China has suspended a policy that would have effectively pushed foreign technology companies out of the country's banking sector, The New York Times reports.

According to The Times, a letter from the Chinese government called for banks to "suspend implementation" of the rules, "which have been at the center of a brewing trade conflict between the United States and China. The rules, put into effect at the end of last year, called for companies that sell computer equipment to Chinese banks to turn over intellectual property and submit source code, in addition to other demands." Read more here.

Financial industries: global outage

Financial markets were thrown into turmoil last Friday as the Bloomberg terminals used by hundreds of thousands of financial industry workers went offline in an unprecedented global outage. According to The Telegraph, the glitch put the Bank of England and European Central Bank on alert, and saw a £3bn auction of UK government debt postponed for hours," The Telegraph reported. "Bloomberg, which prides itself on its resilience and accuracy, blamed the outage on a "combination of hardware and software failures in the network" dismissing the suggestion of cyber-attacks, which have affected other media organizations in the last year."

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
Tompkins Hall, Suite 106
725 23rd Street NW
Washington DC, DC 20052