Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

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

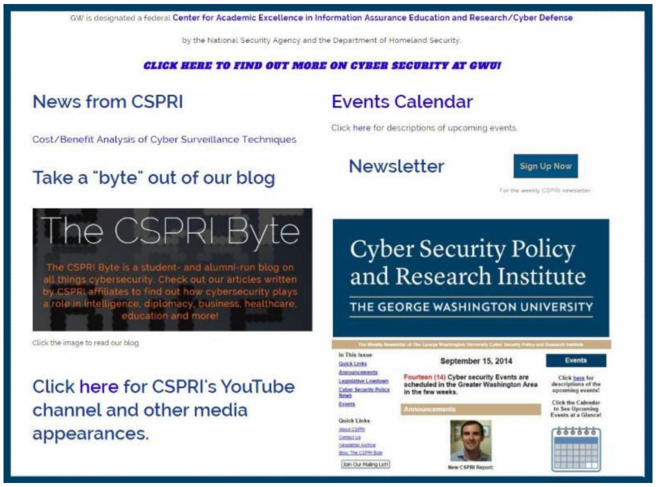
Quick Links

- About CSPRI
- Contact Us
- Newsletter Archive
- Blog: The CSPRI Byte

September 22, 2014

Seven (7) Cyber security Events are scheduled in the Greater Washington Area in the few weeks.

Announcements



GW is designated a federal Center for Academic Excellence in Information Assurance Education and Research/Cyber Defense by the National Security Agency and the Department of Homeland Security.

CLICK HERE TO FIND OUT MORE ON CYBER SECURITY AT GWU!

News from CSPRI

Cost/Benefit Analysis of Cyber Surveillance Techniques

Take a "byte" out of our blog

The CSPRI Byte

The CSPRI Byte is a student- and alumni-run blog on all things cybersecurity. Check out our articles written by CSPRI affiliates to find out how cybersecurity plays a role in intelligence, diplomacy, business, healthcare, education and more!

Click the image to read our blog.

Click here for CSPRI's YouTube channel and other media appearances.

Events Calendar

Click here for descriptions of upcoming events.

Newsletter

Sign Up Now

For the weekly CSPRI newsletter

Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

September 15, 2014

Fourteen (14) Cyber security Events are scheduled in the Greater Washington Area in the few weeks.

Announcements

New CSPRI Report:

Events

Click here for descriptions of the upcoming events!

Click the Calendar to See Upcoming Events at a Glance!

The CSPRI website has been refurbished and now sports a cleaner, more modern look. In addition to providing, as it always has, access to the CSPRI video channel, newsletter archive, and publications by our associated researchers, it also now makes more visible the CSPRI Byte blog (to which all can contribute) and a "one stop shopping" link about all aspects of cybersecurity at GW, including courses throughout the university and the CyberCorps scholarship program. Visit the CSPRI website at: http://www.cspri.seas.gwu.edu/

Events

Click [here](#) for descriptions of the upcoming events!

Click the Calendar to See Upcoming Events at a Glance!

Follow Us

Follow us on Twitter: @gwCSPRI

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

Follow CSPRI Research Scientist, Allan Friedman: @allanfriedman

Legislative Lowdown

Trying to retain cybersecurity experts

-The Senate last week unanimously passed legislation to help the Department of Homeland Security retain cybersecurity experts. According to GovInfoSecuirty, the "Border Patrol Agent Pay Reform Act of 2013" (PDF) -- which incorporates the DHS Cybersecurity Workforce Recruitment and Retention Act - would beef up the cybersecurity workforce at DHS by granting the department secretary personnel authorities similar to those of the defense secretary to hire and retain cybersecurity professionals. "This includes the authority to hire qualified experts in an expedited manner and pay these recruits more competitive salaries as well as furnish benefits and incentives than other employees receive," Eric Chabrow writes. The bill also would require the DHS secretary to report annually on progress in the hiring effort and to ensure adequate transparency and oversight of the recruitment and retention program.

The LEADS Act

-Meanwhile, Senators also introduced a measure designed to give new legal and privacy protections for emails and other documents that consumers often store online. The Law Enforcement Access to Data Stored Abroad (LEADS) Act would require that police obtain a warrant before being able to search through someone's emails and other online documents and would also prevent authorities from using a warrant to nab data stored in servers overseas," writes The Hill. This measure is not the only bill to update the email privacy laws this year. "In the House, more than half the chamber has signed on as a co-sponsor of the Email Privacy Act - which would require a warrant to search emails but does not address the issue of data stored abroad. Yet the bill has remained stuck in committee for more than a year. A similar measure in the Senate has not moved since passing through the Judiciary Committee last spring."

Cyber Security Policy News

Requests for user data

- Government requests for user data are still rising, says Google - up 19 percent in the US from six months ago and 250 percent since the company started publishing the figures in 2009, according to a new report released by the search giant. As Forbes reports, Google "dealt with 32,000 requests over the last six months, an increase of 15 percent over the previous six months and 150 percent more than in 2009. These requests related to around 48,000 accounts."

Smartphone giants changing their policies about giving the government user data

Meanwhile, the latest versions of smartphones produced by both Google and Apple show that both companies are eager to get out of the business of helping the U.S. government easily obtain data from their customers mobile devices. For its part, "Apple won't be turning customer iPhone or iPad data over to law-enforcement officials anymore, even if there is a search warrant," according to the National Journal. "That's because Apple says it won't technically be able to. Apple renewed its privacy vows in an updated privacy policyWednesday night. The update came alongside the rollout of its iOS 8 operating system for the iPhone and iPad, which features enhanced security protections that the tech giant says will effectively make it impossible for it to hand over customers' data to law-enforcement officials."

Likewise, The next generation of Google's Android operating system, due for release next month, will encrypt data by default for the first time, the company said Thursday, raising yet another barrier to police gaining access to the troves of personal data typically kept on smartphones, writes Craig Timberg for The Washington Post. "Google is designing the activation procedures for new Android devices so that encryption happens automatically; only somebody who enters a device's password will be able to see the pictures, videos and communications stored on those smartphones," Timberg writes.

Power grid attacks
-Most of us have at one time or another heard dire warnings about the threat to the U.S. power grid from sophisticated hackers. But according to Politico, there is a growing consensus among security experts that such an attack would not succeed based on cyber capabilities alone. "The half-dozen security experts interviewed for this article agreed it's virtually impossible for an online-only attack to cause a widespread or prolonged outage of the North American power grid," writes Politico's David Perera. "Even laying the groundwork for such a cyber operation could qualify as an act of war against the U.S. - a line that few nation-state-backed hacker crews would wish to cross. Read more here.

This consensus may be cold comfort to those who worry that state-backed Chinese hackers would perhaps be most likely to launch such an attack. According to the Associated Press, China's military hacked into computer networks of civilian transportation companies hired by the Pentagon at least nine times, breaking into computers aboard a commercial ship, targeting logistics companies and uploading malicious software onto an airline's computers, Senate investigators said Wednesday. "A yearlong investigation announced by the Senate Armed Services Committee identified at least 20 break-ins or other unspecified cyber events targeting companies, including nine successful break-ins of contractor networks," the AP's Jack Gillum reports. "It blamed China's government for all the most sophisticated intrusions, although it did not provide any detailed evidence.

Home Depot data breach update
-More than two weeks after independent investigative journalist Brian Krebs broke the news of a credit card breach at Home Depot, the company acknowledged last week that more than 56 million customer debit and credit cards may have been compromised in a data breach that lasted from April to September 2014. Home Depot says it has fully removed the malicious software that stole card data from store cash registers, and that it has completed its rollout of end-to-end encryption to ensure that customer card records are no longer stored or transmitted in plain text within or across its networks. The company hasn't said much about the source of the intrusion, but Krebs writes in a follow-up story that forensic experts have been focusing their attention on the self-checkout lanes within Home Depot stores.

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
304 Staughton Hall
707 22nd St., NW
Washington DC, DC 20052