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

Follow Us

Follow us on Twitter: @gwCSPRI

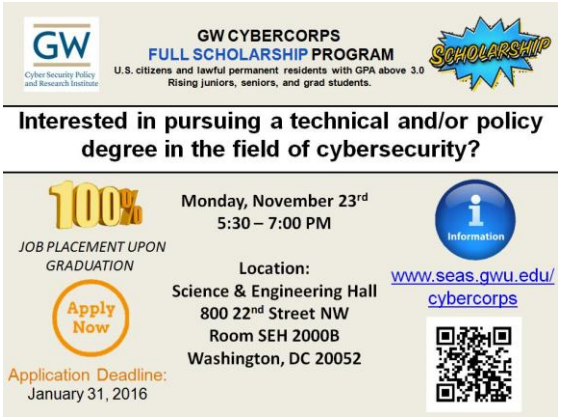
Follow CSPRI Director, Lance Hoffman: @lancehoffman1

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

November 23, 2015

Three (3) events scheduled in the Greater Washington Area in the next few weeks.

CyberCorps Information Session



The application portal is now open for the GW CyberCorps Scholarship Program (2016-2017)!

Come join us **TODAY, November 23rd from 5:30 - 7:00 PM** to get an overview of the scholarship, its benefits, and its requirements. Complete application packages are due by **January 31, 2016.**

Events

November 23
CyberCorps Info Session

December 1
Understanding the IoT Attack Surface

December 1 - 2
Public Sector Cybersecurity Summit 2015

Click here for detailed descriptions

Location:
The George Washington University
Science & Engineering Hall
800 22nd Street NW
Room 2000B
Washington, DC 20052

Click **here** for the CyberCorps webpage.

Legislative Lowdown

-Lawmakers in the House of Representatives last week introduced a bill to crack down on "swatting," an increasingly common and costly hoax in which perpetrators spoof a communication to authorities about a hostage situation or other violent crime in progress in the hopes of tricking police into responding at a particular address with deadly force. "The Interstate Swatting Hoax Act of 2015, introduced by **Rep. Katherine Clark** (D-Mass.) and **Rep. Patrick Meehan** (R-PA), targets what proponents call a loophole in current law, writes Brian Krebs, a journalist who has twice been the target of swatting attacks. "While federal law prohibits using the telecommunications system to falsely report a bomb threat hoax or terrorist attack, falsely reporting other emergency situations is not currently prohibited," reads a statement by the House co-sponsors. To address this shortcoming, the bill "would close this loophole by prohibiting the use of the internet telecommunications system to knowingly transmit false information with the intent to cause an emergency law enforcement response."

Cyber Security Policy News

LabMD Decision

-In a long-running and highly contentious data security enforcement action against LabMD, a small medical testing laboratory, the Federal Trade Commission was handed a stunning defeat. According to the DataSecurityLaw blog, "the ruling came in a 92-page Initial Decision, Chief Administrative Law Judge D. Michael Chappell dismissed the FTC's case against LabMD - after a full administrative trial - based on the Commission's failure to prove it was 'likely' that consumers had been substantially injured in two alleged data security incidents dating back nearly seven years," wrote Craig A. Newman. "This ruling is significant for all organizations that collect and store consumer data - and of particular interest to the 53 companies that, in the face of the FTC's previous inquiries of their data security practices, chose to enter into consent decrees (some with onerous data monitoring provisions) rather than challenge the Commission."

NSA Update
- A federal appeals court last week denied a long-shot attempt to halt the National Security Agency's bulk collection of Americans' phone records. "The Court of Appeals for the D.C. Circuit did not offer any explanation in its widely expected order, which delays a lower court ruling ordering the program to shut down immediately," The Hill reports.

Nevertheless, newly disclosed documents show that the N.S.A. had found a way to create a functional equivalent of a domestic communications-monitoring system that the agency said it had disbanded. The New York Times reports "the shift has permitted the agency to continue analyzing social links revealed by Americans' email patterns, but without collecting the data in bulk from American telecommunications companies - and with less oversight by the Foreign Intelligence Surveillance Court."

OPM Verify
-Anyone who has undergone a federal background check to handle classified information, or is a child or spouse of such an individual, now can visit a Pentagon-hosted website to check if personal data is in the hands of suspected Chinese spies, NextGov reports. The publication notes that on Nov. 17 the U.S. government quietly launched "OPM Verify," a public, self-confirmation tool for the 21.5 million victims of the Office of Personnel hack who have not yet received notification letters or need additional help. Read more here.

US & China: Cyber espionage update
Meanwhile, the U.S. counterintelligence chief said last week he was skeptical China had followed through on recent promises to curb spying on the United States. Earlier this year, President Obama and the Chinese president announced a landmark agreement to rein in cyber espionage attacks from China. But the top defense chief told a briefing last week that he had seen "no indication" from the U.S. private sector "that anything has changed" in the extent of Chinese espionage on the United States. Reuters has the full story.

Pentagon email system: links will become unclickable soon
The Pentagon is tightening up security around email. Federal Computer Week writes that a department-wide policy will soon be in effect to render Web links unclickable in emails to .mil addresses. "The move adds an extra layer of security to anti-phishing measures already in place at the Pentagon," writes Sean Lyngaas. "The new policy, which was coordinated between Hale's office and U.S. Cyber Command, has been rolled out gradually and is already in place for much of the .mil domain."

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