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

Join Our Mailing List!

Follow Us

Follow us on Twitter:
@gwCSPRI

Follow CSPRI Director, Lance Hoffman:
@lancehoffman1

Follow CSPRI Associate Director, Costis Toregas:
@DrCostisToregas

September 28, 2015

Eleven (11) events scheduled in the Greater Washington Area in the next few weeks.

Washington Post Cybersecurity Summit

The Washington Post in partnership with AT&T and The George Washington University Cyber Security Policy and Research Institute will host the Cybersecurity Summit on October 1, 2015 at The Washington Post.

Recent cyber attacks have wreaked havoc on companies and millions of people. Business leaders, lawmakers and security experts will discuss and debate the newest tools for cyber defense and policies to better protect companies, consumers and citizens.

Events

September 29
United States Cybersecurity Policy and Threats

September 29
Outside Perspectives on the Department of Defense Cyber Strategy

September 30
Cyber War: Definitions, Deterrence, and Foreign Policy

September 30
Implementing the Department of Defense Cyber Strategy

October 1
The Washington Post Cybersecurity Summit

October 1
Everything You Need to Know about EMV Chip Card Technology

October 1
The Future of

Location:
The Washington Post
1150 15th Street NW
Washington, DC 20071

Time:
8:30 AM - 11:30 AM

Reserve your seat by clicking **here.**

Cyber Security Policy News

Update: US and China cyber talks
The U.S. and China made progress in talks on curbing cyber espionage last week, reportedly hashing out an agreement by Chinese President Xi Jinping and President Obama. "During Friday's press conference, Obama noted that cybersecurity has been a matter of "serious discussion" between himself and Xi for more than two years, since their bilateral meeting at Sunnylands in California," The National Journal writes. "Though he believes they've made 'significant progress' in figuring out how U.S. and Chinese law enforcement will work together to fight cybercrime, 'the question now is, are words followed by actions?' The president said his administration will be 'watching carefully' to determine the answer to that query. Obama said Xi told him he cannot 'guarantee' the good behavior of all of his citizens, just as Obama can't promise good behavior from all Americans."

Not everyone is convinced the pact will make much of a difference in the status quo. According to The Hill, while at least six members of Congress - Democrats and Republicans - used the phase "step forward" or "first step" to describe the accord, "those same members also said they were "skeptical" that China would adhere to its promise and vowed to closely oversee the agreement's implementation.

Many news publications weighed in on the accord, some supportive and others dismissive. The Wall Street Journalsnubbed the accord as a "mirage" that is full of promises but offers no enforcement. The Christian Science Monitor hailed the deal, saying while President Xi Jinping's public rejection of cyberattacks for commercial espionage has been widely panned, "the deal between Washington and Beijing gives the US a much stronger hand to confront China over its actions in the digital realm." Read more here.

Cyberspying on Iran
Many have charged that the United States doesn't exactly hold the moral high ground when it comes to cyberspying on other nations. According to a top secret document reportedlyobtained by NBC News, an NSA operation against Iran's U.N. delegation to the United States illustrates just how extensive this electronic surveillance can be. "The document shows the U.S. bugged the hotel rooms and phones of then-Iranian President Mahmoud Ahmadinejad and his entire 143-member delegation in 2007, listening to thousands of conversations and learning the 'social networks' of Iran's leadership," NBC reported. "The NSA will

America's Cyber Strategy

October 1-2
Best Practices in Cyber Supply Chain Risk Management

October 2
Conference on Systems Engineering Management & Innovation

October 5-6
ACFCS Cyber Financial Crime Summit

October 16-18
BSides DC Conference

Click here for detailed descriptions

probably spy on foreign leaders like Iranian President Hassan Rouhani during the UN General Assembly in New York this week, applying a "full court press" that includes intercepting cellphone calls and bugging hotel rooms.

A cyber education for the US government
Because so many cyberespionage campaigns begin with a malware-laden or phishing email, security experts across the federal government are working hard to educate federal employees on the dangers of responding to such missives. Now, the Department of Homeland Security's top information security chief says the government should pull the security clearances of any federal employees who fail real-time phishing awareness tests conducted against government workers. DefenseOne explains how Paul Beckman, the Department of Homeland security's chief information security officer, sends his own emails designed to mimic phishing attempts to staff members to see who falls for the scam. "Beckman said he wants to start discussions with DHS' chief security officer - who's responsible for overall personnel security - about incorporating employees' susceptibility to phishing in broader evaluations of their fitness to handle sensitive information," DefenseOne's Jack Moore writes. "Someone who fails every single phishing campaign in the world should not be holding a TS SCI with the federal government," Beckman was quoted as saying.

Update: Foreign Intelligence Surveillance Court
-The shadowy Foreign Intelligence Surveillance Court has appointed its first "friend of the court" (amici curiae) to add an outsider's perspective to the highly secretive process of approving surveillance requests from the government, according to The Intercept. "Preston Burton, a criminal defense attorney known for his work with accused spies, is the first of at least five amici curiae the court must appoint due to a provision in the USA Freedom Act, the surveillance-reform legislative package passed in June," writes Jenna McLaughlin.

Volkswagen: software allowed for incorrect emission numbers
-Volkswagen made international headlines and lost billions in market capitalization last week when it was revealed that the company has been using specialized software to cheat on pollution emission standards for years. But investigative reporter Bob Sullivan argues that the real problem here is the hacking of Volkswagen customers who favored the brand name cars because they claimed to be so advanced in controlling emissions. "Volkswagen allegedly misled consumers by using software to trick emissions testsing procedures," Sullivan writes. "Full emissions controls were turned on during tests, but otherwise off during normal driving. While this alleged evasion of environmental law deserves vigorous prosecution, I keep wondering how consumers will be made whole. After all, their cars' performance was artificially improved by the software, and when recalls are complete, owners' cars will be degraded."

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