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

August 17, 2015

Seven (7) events scheduled in the Greater Washington Area in the next few weeks.

CSPRI Associate Director Costis Toregas discusses cyberdefense

-The federal government is owning up to the modern-day reality that data breaches, no matter the quality of cyberdefenses in place, are inevitable, National Journal observes. "With an eye to future hacks, the government is searching for contractors to keep on call-and it's prepared to pay at least half a billion over the next five years to manage post-breach cleanup," writes Kaveh Waddell. Dr. Toregas discusses the shift in public perception regarding data breaches later in the article: "'It signals an end to the 'It will never happen here because we have good IT teams' syndrome'."

Cyber Security Policy News

NSA update: The role of AT&T
-New documents leaked by National Security Agency whistleblower Edward Snowden to the New York Times appear to confirm what many privacy advocates had suspected for years: That the NSA's ability to spy on vast quantities of Internet traffic passing through the United States has relied on the agency's tight and cooperative relationship with AT&T. "While it has been long known that American telecommunications companies worked closely with the spy agency, newly disclosed N.S.A. documents

Events

August 18
ISSA DC Meetup: Export Controls

August 19
Cyber RiskWednesday

August 19
NovaInfosec Meetup, West

August 20
OWASP NoVA Meetup: Fire Talks

August 26
ISSA Baltimore: Business Continuity

September 1
Mid-Atlantic Security Conference

September 10
Managing Cyber Risk and the Role of Insurance

Click here for detailed descriptions

show that the relationship with AT&T has been considered unique and especially productive," The Times wrote in a story publishedSaturday evening. "One document described it as 'highly collaborative,' while another lauded the company's 'extreme willingness to help.'" Read more here.

Corporate Hacks: $100M in illegal profits

-The Justice Department and securities regulators last week unsealed indictments against a group of men here in the United States and abroad thought to have hacked corporate newswire organizations in a successful campaign to place trades on not-yet-public data. As CNN Money reports, the hackers allegedly made $100 million in illegal profits by gaining access to hundreds of press releases of many leading U.S. companies and trading on the stolen news before it became public. "All told 16 individual stock traders, and 14 businesses profited from the illegal trades, according to civil charges from the Securities and Exchange Commission," CNNwrote. "Nine of those individuals, including the two hackers, also face federal criminal charges."

Grounded planes in Virginia (most likely) due to software failure

-A computer outage in Virginia over the weekend that grounded planes up and down the East Coast was most likely not the result of a cyberattack, the Federal Aviation Administration said. According to The Wall Street Journal, the FAA believes a software failure was the likely culprit behind the cancellation of 476 flights.

Federal agencies & data breaches: A template for contract clauses

Meanwhile, NextGov reports that federal agencies could have a template for data breach contract clauses as early as this fall, according to a detailed draft policy. "Until now, federal standards, White House polices and government-wide information security laws have offered departments and contractors a jumble of information security regulations from which to choose," writes Aliya Sternstein. "The new proposed provisions for 'Improving Cybersecurity Protections in Federal Acquisitions' are meant to ensure government data is kept safe no matter whether it's inside an agency-owned system or a corporate vendor's system. The release, first previewed late last month, still leaves much of the exact language up to each agency's discretion."

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