DREXEL UNIVERSITY
Cybersecurity
Institute

Newsletter | March 2015

UPCOMING EVENTS

AJ Drexel Cybersecurity Institute Symposium: Data Privacy Technology Challenges in 2015

Navigant Consulting, Inc. and the AJ Drexel Cybersecurity Institute Symposium invite you to attend a complimentary 1 hour presentation on Data Privacy Technology Challenges in 2015. We will focus on:

- New Technologies and Data Privacy Challenges
  > Google Glass, GoPro, Smartphones with Camera and Recording capabilities, Smartwatches, Fitbit
- Existing Technologies
  > Social media prevalence (Facebook, Twitter, Instagram)
  > BYOD acceptance, the "connected" workforce and their mobile device expectations (Please send the X-rays to my iPad and I will check them once I get home.)
- App-tly Assessing Risk
  > Dropbox, Snapchat, Yik Yak
  > Gamification
- How do you assess the risk of something without knowing its existence?

Speakers will be Darin Bielby and Stephen Ramey of Navigant

Date: March 26, 2015
Location: Rush Building, Room 014, 30 N. 33rd Street, Philadelphia, PA
Time: 12:00 to 1:00pm

Lunch provided by Navigant

Register:
https://sites.cci.drexel.edu/rsvp/cybersecurity-institute-symposium-3-26-15/

NAVIGANT

AJ Drexel Cybersecurity Institute Symposium: Distinguished Speaker Presentation - Dr. Hal Berghel

The Future of Digital Money Laundering

This talk investigates several types of digital money laundering, characterised by source (failed states, state-aware, keptocratic states, terrorists, extremists, and individuals), means (credit- and debit-card exploits, international funds transfers, klepto-banks, "gift-card" exploits), and purpose (terrorism, narco-trafficking, electronic crime, internet fraud). These catagories are introduced by their identifying events-of-interest. Iimplications on shadow economies, degrees of sophistication, and case studies are discussed. Each crime will be explicitly linked geographically and politically to sources, and may include discussion of actual cases. Several micro- and macro-level mitigation strategies will be discussed.

Date: March 31, 2015
Location: Paul Peck Alumni Center, 3142 Market Street, Philadelphia, PA
Time: 12:00 to 1:00pm

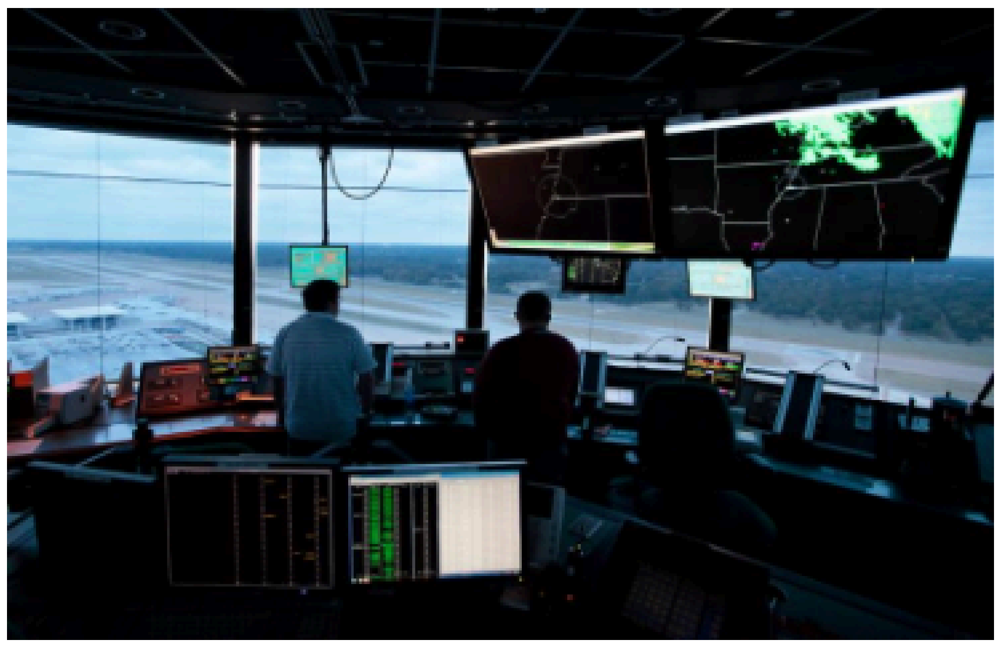
Register:
https://sites.cci.drexel.edu/rsvp/cybersecurity-institute-symposium-3-31-15/

STAY CONNECTED WITH CURRENT EVENTS

http://drexel.edu/cci/about/press-room/events/

CYBERSECURITY SNIPPETS

Government Accounting Office identified weaknesses in our National Airspace Systems to cyber-based threats



While the Federal Aviation Administration (FAA) has taken steps to protect its air traffic control systems from cyber-based and other threats, significant security control weaknesses remain, threatening the agency's ability to ensure the safe and uninterrupted operation of the national airspace system (NAS). These include weaknesses in controls intended to prevent, limit, and detect unauthorized access to computer resources, such as controls for protecting system boundaries, identifying and authenticating users, authorizing users to access systems, encrypting sensitive data, and auditing and monitoring activity on FAA's systems. Additionally, shortcomings in boundary protection controls between less-secure systems and the operational NAS environment increase the risk from these weaknesses.

View full article: http://www.gao.gov/products/GAO-15-221

PENDING PROPOSALS

Cyber-Physical Systems (CPS)

Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components. Advances in CPS will enable capability, adaptability, scalability, resiliency, safety, security, and usability that will far exceed the simple embedded systems of today. CPS technology will transform the way people interact with engineered systems -- just as the Internet has transformed the way people interact with information. New smart CPS will drive innovation and competition in sectors such as agriculture, energy, transportation, building design and automation, healthcare, and manufacturing.

View more: http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286

Secure and Trustworthy Cyberspace (SaTC)

Cyberspace has transformed the daily lives of people for the better. The rush to adopt cyberspace, however, has exposed its fragility and vulnerabilities: corporations, agencies, national infrastructure and individuals have been victims of cyber-attacks. In December 2011, the National Science and Technology Council (NSTC) with the cooperation of NSF issued a broad, coordinated Federal strategic plan for cybersecurity research and development to "change the game," minimize the misuses of cyber technology, bolster education and training in cybersecurity, establish a science of cybersecurity, and transition promising cybersecurity research into practice. This challenge requires a dedicated approach to research, development, and education that leverages the disciplines of mathematics and statistics, the social sciences, and engineering together with the computing, communications and information sciences.

View more: http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709

Cybersecurity Innovation for Cyberinfrastructure (CICI)

Advancements in data-driven scientific research depend on trustworthy and reliable cyberinfrastructure. Researchers rely on a variety of networked technologies and software tools to achieve their scientific goals. These may include local or remote instruments, wireless sensors, software programs, operating systems, database servers, high-performance computing, large-scale storage arrays, and other critical infrastructure connected by high-speed networking. This complex, distributed, interconnected global cyberinfrastructure ecosystem presents unique cybersecurity challenges. NSF-funded scientific instruments are specialized, highly visible assets that present attractive targets for both unintentional errors and malicious activity; untrustworthy software or a loss of integrity of the data collected by a scientific instrument may mean corrupt, skewed or incomplete results. Furthermore, often data-driven research, e.g., in the medical field or in the social sciences, requires access to private information, and exposure of such data may cause financial, reputational and/or other damage.

View more: http://www.nsf.gov/pubs/2015/nsf15549/nsf15549.htm?WT.mc_id=USNSF_25&WT.mc_ev=click

Dr. Steven Weber
Founding Director,
AJ Drexel Cybersecurity Institute
sweber@coe.drexel.edu

Norm Balchunas, Col., USAF (Ret.)
Operations Director,
AJ Drexel Cybersecurity Institute
njb67@drexel.edu

http://cci.drexel.edu/cybersecurity

*If you wish to unsubscribe from this newsletter, please reply directly to the email.