NORTHEASTERN UNIVERSITY CYBERSECURITY AND PRIVACY INSTITUTE

BY THE NUMBERS

170

$ BILLION
expected worldwide spending on Information Security by 2020

1.5

MILLION
number of projected cybersecurity job shortfalls by 2019

Forbes *Cyerbsecurity market reaches $75 billion in 2015; expected to reach $170 billion by 2020*

CYBERSECURITY WORKSHOP FOR BOARDS OF DIRECTORS AND EXECUTIVES

The Northeastern University Cybersecurity and Privacy Institute joins faculty, research scientists, students, government, and industry to be the leader in applied cybersecurity and privacy research and education.

This executive workshop aims to empower board members to develop a cybersecurity vision, and fulfill their responsibilities which include enterprise cybersecurity oversight. It also enables executives and senior management to develop specific cybersecurity strategies and policies, and remain at the forefront of attack vectors awareness and best practices. Running a cybersecurity-aware company requires multi-faceted knowledge spanning cyber insurance/liability, risk assessment with regards to IP theft, cost of breaches including reputation damage, liability with regards to PII/data loss or physical harm in cyber-physical systems, and business interruption. The workshop focuses on industry best practices and can discuss the challenges and benefits of Bring Your Own Devices (BYOD) policies.

Each workshop can be customized to specific audiences and industries like finance, healthcare, or cyber-physical systems, following an agenda template.

TRENDS IN CYBER-ATTACKS AND CYBERSECURITY

- By number (in terms of scale and cost): breaches (statistics by industry), exposed identities, bots, malware, mobile, web, cloud, IoT, ransomware, etc.
- The changing international cyber law landscape (e.g., GDRP, NY DFS Cybersecurity Regs), cyber liability/insurance, outsourcing of security, security-aware decision making and investment prioritization.

ATTACK APPROACHES AND VECTORS

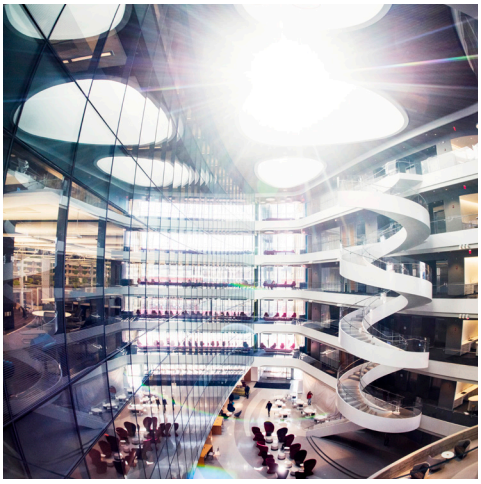
An overview of how existing and emerging attack techniques work. A discussion towards understanding the threats landscape and developing policies that improve the cybersecurity posture of the organization.

- STRIDE model, Phishing, zero-days, ransomware (confluence of cryptocurrencies and privacy infrastructure such as dark web/Tor), mobile & IoT as attack vectors, cloud, supply chain, insider threat, nation state vs. cyber-criminals
- Trends from generic to targeted (Advanced Persistent Threats)

RISKS TO COMPANIES

Covers both direct and indirect risks such as IP theft, data loss/destruction, PII leaks, physical damage, business interruption and being exploited and leveraged against other third parties.

NORTHEASTERN UNIVERSITY CYBERSECURITY AND PRIVACY INSTITUTE



A general view of ISEC as the sun shines through a window in the ceiling on Feb. 15, 2017. Photo by Adam Glanzman/Northeastern University

LEARN MORE ABOUT THE CYBERSECURITY AND PRIVACY INSTITUTE

cyber.ccis.northeastern.edu

LIABILITY AND CYBER INSURANCE

Understanding regulations, laws, and liability, associated with the threats and emerging cyber insurance policies.

STRATEGIES AND BEST PRACTICES FOR SETTING CYBERSECURITY POLICIES AND IMPROVING THE CYBERSECURITY POSTURE

Discuss both general and specific techniques from involvement of CSO/CISO, cybersecurity in the organizational structure, making cyber-security by design a priority for products, setting a cybersecurity culture, relevant and impactful employee education, policies for tracking threats, risks assessment, and planning ahead, assessing BYOD within the context of the company business, and cybersecurity insurance. (creating a written information security program; asset inventory to tier cyber defenses to protect the most valuable; incident response planning)

CASE STUDIES

Deconstructing recent attacks, illustrating failures in policies. Cover a combination of classics (e.g., Target or Cryptolocker), industry specific (e.g., Sony or Mirai IoT), and recent (e.g., Equifax, Whole Foods or Uber). Other potential case studies are dependent on the specific industries and would include classics such as stuxnet/flame for CPS and nation state level of attacks, and the Podesta case for targeted phishing attacks), but also the most recent breaches and attacks.

Northeastern University
Cybersecurity and Privacy Institute

CONTACT

Cybersecurity and Privacy Institute **E** cyberinstitute@ccs.neu.edu **T** 617.373.5204