OVERVIEW

With cyber attacks accelerating, there is an acute shortage of trained cybersecurity professionals and an escalating need for their skills. Our workshops provide the critical knowledge needed to protect an organization’s information assets and systems; make strategic decisions about information security issues including identity theft, computer viruses, and electronic fraud; and provide leadership in these and other strategic efforts.

Northeastern’s cybersecurity workshops help participants build core knowledge surrounding computer system security and network practices; plan and implement security strategies to reduce risk and enhance protection of information assets and systems; understand legal and ethical issues associated with information security, privacy, and digital rights; and enhance communication skills on cybersecurity-related issues. Choose from a spectrum of modules based on current courses or customize based on your industry and audience background.

GENERAL NON-TECHNICAL EMPLOYEE AUDIENCE

Awareness and Best Practices: Duration 2-8 Days

Trains employees to learn about cybersecurity hygiene by demonstrating through examples the implications of failing to follow best practices and security policies. The workshop is supported by carefully selected cases that led to major breaches due to lack of awareness or compliance.

Topics to be covered include anatomy of an attack from reconnaissance to compromise and the role that employees can play in facilitating such attacks or mitigating such attacks, social engineering from the early techniques to the most recent tactics (phishing, pretexting, baiting, quid pro quo, tailgating), sophisticated targeted phishing trends, importance of passwords and multi-factor authentication.

“Cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.” (Cybersecurity Ventures, 2017).

“There will be 3.5 million unfilled cybersecurity positions by 2021.” (Cybersecurity Ventures, 2017).
EXECUTIVES AND BOARD OF DIRECTORS AUDIENCE

Essentials for a Security-Aware Company: Duration 2-8 Days

Enables executives and senior management to remain at the forefront of attack vectors awareness and best practices.

Topics to be covered include threats (stride model), risk assessment and management, technical foundations to security and weakest points (passwords, increasing sophistication of phishing attacks, zero-day attacks, insider threat/BYOD), best practices defense/analysis (overview of defense in depth mechanisms), advanced persistent threats, the dark web, data protection requirements, the changing international cyber law landscape (e.g., GDPR), cyber liability/insurance, outsourcing of security, security-aware decision making, and investment prioritization.

Workshop gives an overview of emerging threats and opportunities (e.g., privacy infrastructure as an attack vector – Bitcoin and Tor, mobile and wireless systems, IoT). Also explores three case studies exposing the multiple facets of cybersecurity threats and levels of sophistication:

- Target (2013): third party vendors as an attack vector
- Mirai (2016): insecure IoT as an attack vector

Other potential case studies can be dependent on the specific industry and would include classics (e.g., stuxnet/flame for CPS and nation state level of attacks, and the Podesta case for targeted phishing attacks), but also recent breaches (e.g., Equifax).

IT SPECIALIST AUDIENCE

Foundations of Secure Enterprise Systems and Trends: Duration 2-8 Days

Provides IT specialists with the knowledge necessary to understand the mechanisms underlying security approaches. A special emphasis is placed on understanding the guarantees and limitations of these schemes as technology evolves. As an example, password cracking has become much easier as a side effect of the emergence of cryptocurrencies miners such as Bitcoin (Antminer can compute over 10 Tera Hashes per second and costs $2K).

Topics include an overview of security fundamentals, the key components (from cryptography building blocks and their limitations, to network security reference architectures) it covers instance topologies, authentication and multi-form factor authentication mechanisms and their limitations against new forms of attacks, web attack vectors, spam/phishing, botnets, and mobile and wireless security. A special focus is placed on practical aspects such as best practices, tools for security assessment, and scripting for automated security tasks such as auditing. More advanced topics include the use of machine learning for security and analysis of emerging threats tactics.

DEVELOPERS AND ARCHITECTS AUDIENCE

Designing and Developing Secure Computer Systems: Duration 2-8 Days

Provides developers and systems architects with the necessary knowledge to analyze and secure existing products and develop future products with security by design. Topics include applied cryptography, network security standards/frameworks and their integration into web/mobile front/back ends, secure software development, operating systems security, Trusted Execution Environments, mobile/wireless security, embedded systems security, IoT security, cloud security, and machine learning for security analysis fundamentals and practice.

Industry-specific topics include Blockchain, public ledgers, and cryptocurrencies (e.g., Bitcoin, Ethereum), and anonymous communications should be of interest to the Fintech industry.

*Certain workshops can be extended in duration (up to 14 weeks) to provide a more comprehensive coverage of subject.*