ISACA®
Trust in, and value from, information systems
Greater Kansas City Chapter

Training Opportunity

Topic: Mobile Security Boot Camp – A Comprehensive Guide to Mobile Security Concepts and Practices

Dates & Times: April 22nd | 8:30 am – 4:30 pm
April 23rd | 8:30 am – 4:30 pm

Location: Sprint Nextel World Headquarters – Overland Park, Kansas
(Additional parking and building information will be provided to registered attendees)

CPE's: 16 Credits

**Please note actual CPE hours granted are dependent upon duration of speaker's presentation and may differ from advertised number of CPE hours.*

Price: ISACA Members Early-Bird: $430 - Available for members today through March 31st.
ISACA Regular Members: $480 - Available for members from April 1st through April 18th.
Non-Members: $640 - Available for non-members today through April 18th.

Course Description

Mobility poses many security-related challenges, including anonymous connections, "always on" connections, clear text network traffic, wireless networks, and many more. Unfortunately, mobile technology usage in the workplace has grown at a rate that far exceeds the training and education necessary to equip information security professionals to adequately protect their organizations and their end users from mobile-related threats. These professionals are further challenged by the fact that mobile devices are finding their way into the workplace, whether or not the business is ready for them.

This two-day seminar is designed to provide the knowledge and experience you need in order to enable your organization to securely embrace, deploy, and manage mobile devices and applications. Through both discussion and hands-on exercises you will gain specialized knowledge of mobile technology security. We will cover mobile computing fundamentals, security settings for varying device types, assessing mobile computing risks, developing mobile policies, procedures, & standards, auditing mobile devices, deploying & managing a Mobile Device Management (MDM) solution, attacking and defending mobile devices & applications, and mobile device forensics.

- Mobile Computing Fundamentals
  - Defining mobile computing
  - Network services and connections
  - Mobile device configuration management
  - Jailbreaking and rooting
  - App stores
  - Mobile Device Management (MDM)
- Securing Mobile Devices
  - Essential security controls for all mobile devices
  - iOS security configurations
  - Android security configurations
  - Blackberry security configurations
  - Windows Mobile security configurations
  - Interactive hands-on exercises
- Assessing and Managing Mobile Risks
  - Risk management methodologies
  - Bring Your Own Device (BYOD)
  - Physical, Network and Device risks
  - Legal and regulatory risks
  - Training and education
- Mobile Policies, Procedures, and Standards

    - Generating a mobile computing policy
    - Developing mobile computing standards
    - Essential mobile computing procedures
    - Updating related policies, procedures, and standards
    - Interactive policy development workshop
- Auditing Mobile Devices
    - Applying the ISO/IEC 27000 series of controls to mobile devices
    - How to determine what you will audit
    - Developing an internal auditing program
    - Tools to support the mobile device audit process
- Deploying and Managing an MDM Solution
    - Planning an MDM deployment
    - Related infrastructure considerations
    - Related support and staffing considerations
    - Survey of MDM solutions currently in the market
    - Hands-on device provisioning and de-provisioning exercises
- Attacking and Defending Mobile Devices and Applications
    - Understanding the Penetration Testing Execution Standard (PTES)
    - Applying the PTES
    - An attacker's perspective
    - Configuring mobile devices and applications to resist attacks
    - Related detection and response tools and procedures
    - Fundamental mobile forensics technique
- Mobile Forensics Workshops
    - Understanding the forensic process
    - Mobile device types / Evidence types /Data acquisition types
    - Anti-forensics
    - Online forensics tools and techniques

Registration
Registration is available online: http://www.isaca-kc.org/meetingReg.php
Registration fees must be paid promptly following registration to secure your seat and course materials, if you are paying by check. Credit Card payment must be made at the time of registration.

Registration Includes
Course material and a $20 daily food voucher to be used the day of issuance at the on-site cafeteria for breakfast, lunch and / or snacks.

Cancellation Policy
The Greater Kansas City Chapter of ISACA reserves the right to cancel the training seminar if the instructor is unable to attend, the facilities are not available, minimum number of registered attendees is not met, or other unforeseen circumstances arise. If this occurs, a reasonable effort will be made to reschedule the seminar, or refunds will be issued. If a registrant cannot attend the seminar, the Chapter requests an email notification by April 1st. Refunds will not be granted for cancellation requests received after this date. Generally, the Chapter does not charge registrants a cancellation fee or penalty. Substitution of another individual for a confirmed registrant will be accepted at any time prior to the date of the event.

Speaker
Jerod Brennen, CISSP (Senior Instructor MIS Training Institute)

Jerod Brennen is the CTO and Principal Security Consultant with Jacadis, an award-winning security solutions and services provider. Jerod is responsible for performing security assessments, penetration tests, and security architecture reviews, as well as evaluating security technologies on behalf of Jacadis clients. He applies his hands-on experience in support, management, and budgeting roles to help Jacadis clients identify and implement reasonable and appropriate security controls to meet their security and compliance obligations.

Jerod has over a decade of IT, information security, and compliance experience. Prior to joining Jacadis, Jerod spent years as an Information Security Specialist with American Electric Power, one of the largest electric utilities in the U.S., before moving to Abercrombie & Fitch (A&F), a multibillion dollar international luxury retailer. At A&F, Jerod built out and managed the information security program. His team was tasked with security operations, PCI and SOX compliance, and identity and access management.

Jerod's approach to information security has two key tenets: you shouldn't be afraid to void warranties, and you shouldn't need to bypass security to get your work done.