CYBERSECURITY FUNDAMENTALS WORKSHOP

Title: Cybersecurity Fundamentals Workshop

Length: 2 Days

Level: Beginner – intermediate

Target audience:

- Zero to three years cybersecurity experience.
- Audit, risk, compliance, information security, government and legal professionals with a familiarity of basic IT/IS concepts who:
    - are new to cybersecurity
    - are interested in entering the field of cybersecurity
    - are interested in the ISACA Cybersecurity Fundamentals Certificate
- This course would be appropriate for students and recent graduates

Course Description:

Why become a cybersecurity professional? The protection of information is a critical function for all enterprises. Cybersecurity is a growing and rapidly changing field, and it is crucial that the central concepts that frame and define this increasingly pervasive field are understood by professionals who are involved and concerned with the security implications of Information Technologies (IT). The CSX Fundamental Course is designed for this purpose, as well as to provide insight into the importance of cybersecurity, and the integral role of cybersecurity professionals. This course will also cover four key areas of cybersecurity: 1) cybersecurity architecture principles, 2) security of networks, systems, applications and data, 3) incident response, and 4) the security implications of the adoption of emerging technologies. Designed as a foundational course, it will also prepare learners for the CSX Cybersecurity Fundamentals Exam.

Learning Objectives:

After completing this workshop, you will be able to:

- Understand basic cybersecurity concepts and definitions
- Identify Cybersecurity roles
- Understand basic security architecture principles
- Understand malware analysis concepts
- Recognize the techniques for detecting host-and-network-based intrusions via intrusion detection technologies
- Understand vulnerability assessment management
- Recognize penetration testing phases

- Understand high level network security, including remote access technology and systems administration concepts
- Understand system hardening and virtualization
- Recognize system lifecycle management principles
- Review the OWASP top ten
- Differentiate between events and incidents
- Define types of incidents and identify elements of an incident response plan
- Be aware of the basic procedures for processing digital forensic data
- Recognize new and emerging information technology, and identity the associated security implications

Note:

This course is not designed to cover all knowledge areas that will be tested during the Cybersecurity Fundamentals Certificate Exam. Therefore, it is recommended that you understand the following concepts prior to taking the exam. Being familiar with these items will also provide you with greater understanding of the materials presented during the workshop:

- Security architecture principles and frameworks (i.e. SABSA, Zachman, TOGAF, etc.)
- OSI model
- TCP/IP
- General firewall features, types, issues, and platforms
- Networking (i.e. ports, protocols, VPNs, etc.)
- Application security
- Risk assessments
- Business continuity plans (BCP)
- BYOD
- Cloud computing
- Mobile technology risks

Course Outline:

1. Cybersecurity Introduction & Overview
    a. Introduction to Cybersecurity
    b. Difference between Information Security & Cybersecurity
    c. Cybersecurity objectives
    d. Cybersecurity roles
2. Cybersecurity Concepts
    a. Risk
    b. Common attack types & vectors
    c. Policies & procedures
    d. Cybersecurity controls
3. Security Architecture Principles
    a. What is security architecture
    b. The OSI model

    c. Defense in depth
    d. Firewalls
    e. Isolation & segmentation
    f. Monitoring, detection, & logging
    g. Cryptography fundamentals & applications
4. Security of Networks, Systems, Applications, & Data
    a. Process controls – risk assessments
    b. Process controls – vulnerability management
    c. Process controls – penetration testing
    d. Network security
    e. Operating system security
    f. Application security
    g. Data security
5. Incident Response
    a. Event vs. incident
    b. Types of incidents (categories)
    c. Security incident response
    d. Investigations, legal holds, & preservation
    e. Forensics
    f. Disaster recovery
6. Security Implications & Adoption of Evolving Technology
    a. Current threat landscape
    b. Advanced persistent threats (APTs)
    c. Mobile technology – vulnerabilities, threats, & risk
    d. Consumerization of IT & mobile devices (BYOD)
    e. Cloud computing