Cybersecurity Fundamentals Course (Four-Day)

Why become a cybersecurity professional? The protection of information is a critical function for all enterprises. Cybersecurity is a growing and rapidly changing field that focuses on the protection of information assets that are embedded in internetworked information systems. Given today's technological advances, professionals who are involved information technologies must be knowledgeable about the central concepts and security implications that frame and define this increasingly all-pervasive field.

The CSX Fundamentals Course is designed to provide an overview of this material, as well as to offer 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 Fundamental Exam.

Who Should Attend This Course?

The target audience for this course includes individuals with the following qualifications:

- Audit, risk, compliance, information security, government and legal professionals with a familiarity of basic information technology and information systems concepts, who are:
  - New to cybersecurity
  - Interested in entering the field of cybersecurity
  - Interested in the ISACA Cybersecurity Certification
- Students and recent graduates interested in the field of cybersecurity
- Individuals with zero to three years cybersecurity experience

Pre-Assessment

A pre-assessment provided to attendees will assist the instructor in determining the baseline knowledge of participants, as well as any necessary demographic information. Results from the pre-assessment should be used to help focus lecture and activities to be most meaningful to all participants. The pre-assessment should include questions regarding:

- Level and years of information technology-related experience or other practical experience
- Knowledge or experience in the area of information security and cybersecurity
- Current title and role
- Enterprise specifics:
- Domestic or international
- Size and number of employees
- Industry
- Region (US or non-US)
- Educational background
- Degree in cybersecurity or a related field (if so, what)?
- What university did they attend?

Course Learning Objectives

After completing this course, attendees will be able to:

- Identify key concepts and terminology in cybersecurity.
- Define the key concepts, roles and domains of cybersecurity.
- Identify the various types of cybersecurity architecture.
- Identify the key components of securing networks, systems and applications and data.
- Identify and incident and outline the phases of incident response.
- Identify the implications for adaption of evolving technology.

Course Outline

Day One

Activity 1: Icebreaker/Introductions

1. Cybersecurity Introduction and Overview

1.1. Introduction to cybersecurity

1.2. Difference between information security and cybersecurity

1.3. Cybersecurity objectives

1.4. Cybersecurity roles

1.5. Cybersecurity domains

2. Cybersecurity Concepts

2.1. Risk

2.2. Common attack types and vectors

2.3. Policies and procedures

2.4. Cybersecurity controls

Day Two

3. Security Architecture

3.1. Overview of security architecture

3.2. The OSI model

3.3. Defense in depth

3.4. Information flow control

3.5. Isolation and segmentation

3.6. Logging, monitoring and detection

3.7. Encryption fundamentals, techniques and applications

Course Outline (continued)

Day Three

4. **Security of Networks, Systems, Applications and Data**

   4.1. Process controls—Risk assessment

   4.2. Process controls—Vulnerability management

   4.3. Process controls—Penetration testing

   4.4. Network security

   4.5. Operating system security

   4.6. Application security

   4.7. Data security

Day Four

5. **Incident Response**

   5.1. Event vs. incident

   5.2. Security incident response

   5.3. Investigations, legal holds, and preservation

   5.4. Forensics

   5.5. Disaster recovery and business continuity

6. **Security Implications and Adoption of Evolving Technology**

   6.1. Current threat landscape

   6.2. Advanced persistent threats (APTs)

   6.3. Mobile technology—Vulnerabilities, threats, and risk

   6.4. Consumerization of IT and mobile devices

   6.5. Cloud and digital collaboration

7. **Course Summary**