Cybersecurity Fundamentals

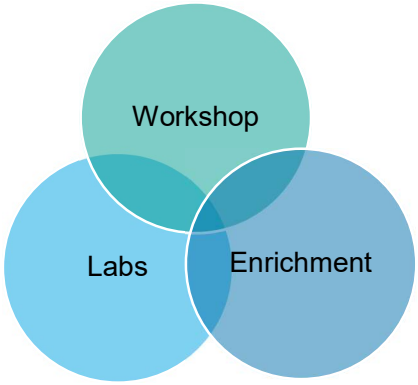
Course Overview

This 15-session course introduces you to cybersecurity, a growing and rapidly changing field that is becoming increasingly vital to business survival, job stability, and national security. Cybersecurity demands skilled professionals who possess the knowledge, skills, and ability to address the evolving threat landscape. Each session is approximately two hours long.

Course Approach

The content is laid out in a workshop format structured to provide a holistic learning experience leading to proficiency. This is not a self-paced course. This course also contains case study material based on real-life scenarios but does not reference any particular company or situation.

Content Types



There are three content types in this course:

Workshop: Main course content, typically in a slide deck or recorded, lecture-style format.

Enrichment: Additional content provided for the learning experience in the course. These are items that, while not required, may provide a bigger picture or more context around content presented in the course. These are content elements including (but not limited to) journal articles, podcasts, whitepapers, webinars or links from other trusted sources.

Labs: This course has a performance-based lab component that is highly recommended for learners to complete. Completion of the labs is in addition to the instructor led course and will reinforce the learning in a hands-on, skill building approach.

The Cybersecurity Fundamentals Certificate Exam assesses and affirms both knowledge and the ability to perform IT-related tasks that the real-world workplace demands. The exam includes multiple choice questions and specific skills that are assessed in a virtual lab environment.

Access to the labs are available through the ISACA PERFORM learning experience platform.

Session 1 – Introduction to Cybersecurity

Learning Objectives:

- Identify the need for cybersecurity.
- Explain cybersecurity concepts.
- Identify the need for cybersecurity professionals.
- Identify main components of telecommunications technologies.
- Differentiate between types of security.

Session topics:

- 1.1 Overview
- 1.2 What is Security?
- 1.3 Types of Security

Enrichment:

- Getting the Basics of Cybersecurity Right, ISACA Journal (https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/getting-the-basics-of-cybersecurity-right)

Session 2 – Cybersecurity and Privacy

Learning Objectives:

- Identify differences between information technology systems and specialized systems.
- Discuss enterprise cybersecurity roles and responsibilities.
- Define governance, risk management and compliance (GRC).
- Recognize relationships between various security components.
- Define privacy.
- Distinguish between privacy and security.

Session topics:

- 1.4 Specialized Systems
- 1.5 Roles and Responsibilities
- 1.6 Governance, Risk Management and Compliance
- 1.7 Cybersecurity Governance
- 1.13 Privacy
- 1.14 Privacy vs. Security

Session 3 – Service Disruption and Cybersecurity

Learning Objectives:

- Identify and discuss common causes of enterprise service disruption.
- Explain business continuity planning.

- Describe the relationship between business continuity planning (BCP) and disaster recovery (DR).
- Explain information security objectives.

Session topics:

- 1.8 Resilience
- 1.9 Business Continuity and Disaster Recovery
- 1.10 Business Impact Analysis
- 1.11 Recovery Concepts

Session 4 – Threat Landscape

Learning Objectives:

- Define cyberrisk.
- Define key terms associated with risk.
- Identify and describe threats to enterprises.
- Explain the process of threat modeling.
- Identify common types of vulnerabilities.
- Identify common threat agents
- Describe the recent trends in the cybersecurity landscape.

Session topics:

- 1.4 Specialized Systems
- 1.5 Roles and Responsibilities
- 1.6 Governance, Risk Management and Compliance
- 1.7 Cybersecurity Governance
- 1.13 Privacy
- 1.14 Privacy vs. Security

Session 5 – Cyberattacks

Learning Objectives:

- Identify attributes of cyberattacks.
- Explain the cyberattack process.
- Identify cybersecurity attack models.
- Identify common cyberattacks.

Session topics:

- 2.5 Attack Attributes
- 2.6 Attack Process
- 2.7 Malware and Attacks

Enrichments:

- Cybersecurity Takedowns, ISACA Journal (https://www.isaca.org/resources/isaca-journal/issues/2019/volume-6/cybersecurity-takedowns)

Session 6 – Risk Management

Learning Objectives:

- Describe the IT risk management life cycle.
- Explain the supply chain considerations for risk management.
- Elaborate the Risk Management Life Cycle.
- Describe Risk Identification process.
- Explain Risk Assessment and Risk Response.
- Describe Risk and Control Monitoring.
- Narrate the uses of Risk Assessment results.

Session topics:

- 2.8 Risk Assessment
- 2.9 Supply Chain Considerations
- 2.10 Risk Management Life Cycle
- 2.11 Managing Risk
- 2.12 Using the Results of Risk Assessments

Enrichments:

- Understanding Cybersecurity Risk, ISACA Journal (https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/understanding-cybersecurity-risk)

Session 7 – Securing Assets

Learning Objectives:

- Distinguish categories of resources used to identify and classify risk.
- Explain system hardening.
- Summarize data protection means and methods.

Session topics:

- 3.1 Risk Identification, Standards, Frameworks and Industry Guidance
- 3.3.8 Endpoint Security
- 3.3.9 System Hardening
- 3.3.10 Logging, Monitoring and Detection
- 3.3.13 Data Security

Session 8 – Security Architecture

Learning Objectives:

- Explain the concept of security architecture
- Describe security perimeter
- Identify components of a security architecture
- Recognize the various security architecture frameworks
- Compare security models

Session topics:

- 3.2 Architecture, Models, and Frameworks

Enrichment:

- Disaster Recovery, ISACA Journal (https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/getting-the-basics-of-cybersecurity-right

Session 9 – Security Controls

Learning Objectives:

- Explain defense in depth.
- Compare traditional security and assume-breach philosophies.
- Identify three main types of security controls.
- Distinguish types of logical access controls.
- Identify and explain types of administrative controls.
- Explain each component of authentication, authorization and accounting (AAA).

Session topics:

- 3.3 Security Controls (3.3.1 to 3.3.6)

Session 10 – Network Security

Learning Objectives:

- Describe the various network security techniques
- Explain methods to achieve isolation and segmentation
- Identify network security hardware
- Distinguish types of firewalls

Session topics:

- 3.3.7 Network Security

Session 11 – Application and Cloud Security

Learning Objectives:

- Recognize system life cycle management principles, including software security and usability.
- Identify and analyze cloud service models.
- Explain the cloud deployment models
- Discuss risk associated with cloud computing.

Session topics:

- 3.3.11 Application Security
- 3.3.12 Cloud Security

Enrichment:

- Pizza as a Service 2.0, Article (https://medium.com/@pkerrison/pizza-as-a-service-2-0-5085cd4c365e)

Session 12 - Software Management and Encryption

Learning Objectives:

- Identify elements of cryptographic systems.
- Explain the encryption techniques and applications.
- Identify and discuss key systems.

Session topics:

- 3.3.14 Configuration Management
- 3.3.15 Change Management
- 3.3.16 Patch Management
- 3.3.17 Encryption Fundamentals, Techniques and Applications

Session 13 – Introducing Security Operations

Learning Objectives:

- Discuss security operations center (SOC) deployment models.
- Identify common SOC functions, roles and responsibilities.
- Identify vulnerability assessment tools, including open source tools and their capabilities.

Session topics:

- 4.1 Security Operations

Session 14 – Testing Technologies and Security Tools

Learning Objectives:

- Differentiate between vulnerability scanning and penetration testing.
- Discuss common phases of penetration testing.
- Identify and use common cybersecurity tools.
- Discuss the components that aid cybersecurity monitoring and detection.
- Explain the basic concepts, practices, tools, tactics, techniques and procedures for processing digital forensic data.
- Identify common antiforensic tactics and techniques.

Session Topics:

- 4.2 Tool and Technologies (Monitoring, Detection, Correlation)
- 4.4 Forensics

Enrichment:

- Using Red Teaming to Improve Your Security, Podcast (https://www.isaca.org/resources/news-and-trends/isaca-podcast-library/using-red-teaming-to-improve-your-security)

Session 15 – Handling Security Incidents

Learning Objectives:

- Recognize incident response and handling methodologies.
- Distinguish between an event and an incident.
- Discuss the elements of an incident response plan (IRP).

Session Topics:

- 4.3 Incident Handling

Practice Labs:

- SQL Injection
- Windows Event Monitoring & Defender
- Threat Removal
- Threat Detection
- File Permissions on Windows and Linux
- Forensics: File Recovery, Baselining with Lynis
- Scanning Ports and Utilizing SSH
- Windows and Linux OS Firewalls