Cybersecurity Auditing in an Unsecure World

About This Course

Course Description
$5.4 million — that’s the average cost of a data breach to a U.S.-based company. It’s no surprise, then, that cybersecurity is a hot topic and a major challenge in internal auditing today. Cybersecurity is as much of a business risk as it is a security one, making it critical for internal auditors to develop the skill set needed to take on these challenges.

In this course, you will develop an understanding of cybersecurity concepts that can be used to facilitate integrated audit efforts within your organization. Developed with and facilitated by leading industry experts, this course will examine preventive, detective, and corrective controls, and how to apply the audit process to a cloud environment. You will also be exposed to the mobile environment and cyber standards, as well as learn how to audit common security solutions.

This course is designed for internal auditors involved in IT audits or those involved in audit activities that require an understanding of how to manage the impact of cybersecurity events on business risks.

Course Objectives
- Define cybersecurity from an audit perspective, including an understanding of its scope, limitations, and how to measure effectiveness.
- Identify the purpose of preventive, detective, and corrective controls.
- Understand cyber liability insurance and its impact on cybersecurity.
- Understand cyber standards, state notification laws, and how they affect an organization.
- Understand how to assess an organization’s cyber capabilities from an attacker perspective, using threat modeling.
- Assess cybersecurity risks and controls related to using cloud providers or third-party vendors.
Course Topics

Overview of Cybersecurity
- What is Cybersecurity?
  - Definition of Cybersecurity
  - Misconceptions
  - Cybersecurity Evolution
  - Types of Risks and Controls

Preventive Controls
- Purpose of Preventive Controls
- Types of Attackers
- Threat Models
- Anatomy of a Breach
  - “The Breach Quadrilateral”
- Preventing Cyber Incidents
  - Network Controls (Internal and External)
  - Domain and Password Controls
  - Access Methods and User Awareness
  - Application Security
  - Secure Software Development Lifecycle (SSLDC)
  - Data Controls
  - Host and Endpoint Security
  - Vulnerability Management
  - Security Testing

Detective Controls
- Purpose of Detective Controls
- Detecting Cyber Incidents
- Log Detail Concepts
- Security Information and Event Management (SIEM)
  - Traditional Silo-Specific Model
  - Alert Rules
  - Correlation Rules
- Data and Asset Classification
Corrective Controls

- Purpose of Corrective Controls
- Incident Response and Investigation Process
  - Incident Scoping and Evidence Preservation
  - Forensic Analysis
  - Defining Period of Compromise
  - Evaluating Risk of Harm to Information
  - Production of Data for Review
- Corrective Actions
  - Incident Response Tasks
  - Identifying Potential Evidence Sources
- Detection Dependencies
  - Understanding the Scope of the Breach
  - Identifying Compromised Systems and Applications
  - Determining Scope of Information to Be Preserved
  - Preparing for Future Media and Legal Inquiries

Cybersecurity Risks, Cyber Liability Insurance, and State Notification Laws

- Mitigating Costs and Risks
  - Organizational Programs
  - Specific Preparation Tasks
  - Response Documentation
  - Data Segregation
  - Network and Application Patch Management
  - Backup and Archiving Solutions
  - Enterprise Monitoring Solutions
- Insurance Overview
  - Security and Privacy Liability
  - Regulatory Defense and Penalties
  - Payment Card Industry Fines and Penalties
  - Breach Response Costs
- Notification Law Overview
  - Who the Laws Apply To
  - What the Laws Do
Applying the Audit Process to a Cloud Environment or Third-Party Service Provider

- Cloud Providers
  - Assessing the Provider
  - Evaluating the Data
  - Selecting the Provider
  - Annual Assessment/Service Organization Control (SOC) Reports
- Third-Party Service Providers
  - Contractual Risks
  - Vendor Management Program
  - Individual Contractor Management/Security

The Mobile Environment, Bring Your Own Device (BYOD), and Social Networking

- Mobile Computing Risks, Control Activities, and Incident Management
- BYOD Risks, Control Activities, and Incident Management
- Social Networking Risks, Control Activities, and Incident Management

Cyber Standards

- Common Standards
  - ISO 2700 Series
  - NIST sp800 Series
- Common Uses
  - Completeness vs. Correctness
  - Governance Mapping for Regulatory and Insurance Needs

Auditing Common Security Solutions

- SEIM
- Data Loss Prevention (DLP)
- Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)
- Network Segmentation
- Encryption
Course Information

Course Duration: 2 Days

CPE Hours Available: 16

Knowledge Level: Basic

Field of Study: Information Technology

Prerequisites: None

Advance Preparation: None

Delivery Format: eLearning (Group-Internet-Based); On-site Training (Group-Live); Seminar (Group-Live)