CYBERSECURITY AWARENESS

PROFESSIONAL CERTIFICATION

CAPC™ Versión 072024

CertiProf®

Cybersecurity Awareness

Syllabus V072024

Introduction

Cybersecurity awareness is crucial in today's digital age, where the increasing threat landscape poses significant risks to individuals and organizations alike. Understanding the principles of cybersecurity helps protect sensitive information, maintain system integrity, and ensure the availability of critical resources. By recognizing common threats such as malware, phishing, and social engineering, and implementing protective measures like strong passwords, multi-factor authentication, and regular software updates, individuals and organizations can safeguard their digital assets. Cybersecurity awareness also involves staying compliant with regulatory requirements, establishing robust security policies, and fostering a security-conscious culture through ongoing training and education. Join us in enhancing your cybersecurity knowledge and skills to create a safer digital environment.

Learning Objectives:

- Recognize the increasing threat landscape and its economic impact.
- Comprehend the legal requirements and the significance of cybersecurity in protecting sensitive information.
- Grasp fundamental cybersecurity principles, including the CIA Triad (Confidentiality, Integrity, and Availability).
- Distinguish between cybersecurity and information security and understand their integration.
- Learn to establish strong password policies, utilize multi-factor authentication, and ensure regular software updates.
- Understand device and network protection, secure email practices, and information security measures.
- Identify various types of threats such as malware, phishing, social engineering, and DoS/DDoS attacks.
- Develop skills in vulnerability management, including identifying, assessing, and mitigating risks.
- Master the protocols for detecting, responding to, and recovering from cybersecurity incidents.
- Understand the importance of documentation and reporting in maintaining security and compliance.
- Establish and enforce comprehensive security policies within an organization.
- Stay compliant with regulatory standards such as GDPR and HIPAA through regular audits and improvements.
- Ensure secure remote work practices and understand the role of leadership in cybersecurity strategy.
- Conduct thorough risk assessments to identify and prioritize cybersecurity risks.
- Learn the basics of identity management and access controls, including tools like single sign-on (SSO) and multi-factor authentication (MFA).
- Implement best practices for managing identities and access through regular reviews and audits.

Target Audience:

- Network administrators, system administrators, and IT support staff who need to enhance their cybersecurity knowledge and skills.
- Senior management, project managers, and department heads responsible for implementing and overseeing cybersecurity policies and strategies.
- Professionals tasked with ensuring that their organizations adhere to regulatory standards and cybersecurity best practices.
- Human resources staff who need to understand cybersecurity to better train and support employees in maintaining secure practices.
- All employees within an organization who need to understand basic cybersecurity principles and practices to protect themselves and their company.
- Individuals looking to enter the cybersecurity field or enhance their understanding of cybersecurity as they transition into new careers.

Prerequisites:

- Therea are no formal prerequisites for this certification.

Training:

- Type of Course: Professional
- Certification Code: CAPC™
- Expiration: 3 years

Certification Exam:

- Format: Multiple Choice
- Questions: 40
- Language: Spanish, English, and Portuguese
- Duration: 60 minutes
- Open Book: No
- Delivery: This exam is available online
- Supervised: It would be at the Partner's discretion

Content

Module 1: Introduction to Cybersecurity

- **Duration: 1 hour**
- **1.1 Welcome and Course Objectives**
  - Instructor introduction.
  - Course objectives and expectations.
- **1.2 Basic Concepts of Cybersecurity**
  - What is cybersecurity?
  - Importance of cybersecurity in today's environment.
  - Differences between cybersecurity and information security.
- **1.3 Principles of Cybersecurity**
  - Confidentiality, Integrity, and Availability (CIA).
  - Defense-in-depth principles.
  - Best practices in information security.

Module 2: Common Threats and Vulnerabilities

- **Duration: 1 hour**
- **2.1 Types of Threats**
  - Malware: viruses, worms, trojans, ransomware.
  - Phishing and social engineering attacks.
  - Denial-of-Service (DoS and DDoS) attacks.
- **2.2 Common Vulnerabilities**
  - Software and hardware vulnerabilities.
  - Configuration issues.
  - Human errors and their impact on security.

Module 3: Protective Measures and Best Practices

- **Duration: 1 hour**
- **3.1 Device and Network Protection**
  - Use of antivirus and security software.

- Secure configuration of Wi-Fi networks.
- Importance of updates and security patches.

- **3.2 Personal and Professional Information Security**
  - Creating and managing strong passwords.
  - Use of Multi-Factor Authentication (MFA).
  - Secure email and attachment management.
- **3.3 Safe Internet Browsing**
  - Identifying secure websites.
  - Preventing online fraud.
  - Use of VPNs and other privacy tools.

Module 4: Incident Response and Best Practices

- **Duration: 1 hour**
- **4.1 Incident Detection and Response**
  - What to do in the event of a security incident.
  - Response and recovery protocols.
  - Importance of documentation and incident reporting.
- **4.2 Continuous Awareness and Training**
  - Building a security culture within the organization.
  - Ongoing awareness and training programs.
  - Additional resources and next steps.

Module 5: Policies and Compliance

- **Duration: 1 hour**
- **5.1 Security Policies**
  - Developing and implementing security policies.
  - Acceptable use policies.
  - Information access policies.
- **5.2 Regulatory Compliance**
  - Introduction to cybersecurity laws and regulations.
  - Compliance with standards like GDPR, HIPAA, etc.
  - Security audits and controls.

Module 6: Cybersecurity in the Corporate Environment

- **Duration: 1 hour**
- **6.1 Remote Work Security**
  - Best practices for secure remote work.
  - Use of personal devices and BYOD.
  - Ensuring secure communication and collaboration online.
- **6.2 Cybersecurity for Executives and Leaders**
  - Responsibilities of leaders in cybersecurity.

- Integrating cybersecurity into business strategy.
- Risk assessment and informed decision-making.

- **6.3 Introduction to Identity and Access Management (IAM)**
  - Basic concepts of IAM.
  - IAM tools and technologies.
  - Best practices for managing identities and access.