Certificate in Cybersecurity

Cybersecurity, also known as Information Security, protects data and personally identifiable information from malicious attacks, theft, and destruction. Failures of cybersecurity policies in large corporations and governmental agencies have gained significant visibility and negative publicity recently. As data storage increases and hackers become more sophisticated, the need for cybersecurity is more significant than ever.

Courses Included in this Certificate

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Security and Risk Management

This course covers the role of governance and risk management in information security. It looks at the policies and standards that are needed to operate an effective information security function and to oversee good information security practices. The course also includes a look at how modern organizations manage information security risks and how to conduct a risk analysis. It concludes by examining the process for providing information security training and education. This course requires some basic understanding of IT concepts.

Learning Outcomes

- Discuss the concept of security governance and understand the job of overseeing data security
- Describe the role of policy and procedure documents in information security
- Understand the key principles and terminology of information security governance and risk management
- Discuss different management practices for overseeing an effective information security function
- Identify common information security risks and threats
- Describe the process for conducting a risk assessment
- Understand the data classification process and properly classify data according to security needs
- Explain the process for providing information security training and education

Asset Security

Companies must protect their assets. Just as locks are placed on doors to protect physical assets, electronic and data assets must also be guarded. Asset security involves the full support of everyone in an organization, from corporate-level personnel down to front-line employees. Various security controls will be described that help protect privacy and data leakage prevention (DLP). Although it is unnecessary, having some foundation in IT concepts helps take this course.

Learning Outcomes

- Understand the role of asset security and discuss its key themes
- Discuss the information life cycle and explain how information and data are classified
- Compare the various titles and roles of those involved with information security within an organization
- Learn about data and information privacy and how to protect privacy
- Compare different data retention and destruction methods
- Explain several methods for countering data leakage

Security Architecture and Engineering

This course contains an introduction to the key concepts of cryptography and security engineering. It examines the role of encryption in information security and considers common encryption methods. In addition, the course discusses ciphers, their substitutes, and how they work. Public key infrastructure and management is also covered. This course requires a basic understanding of IT concepts.

Learning Outcomes

- Understand how cryptography works and its role in information security
- Compare and contrast different ciphers and explain how they work
- Create substitution ciphers and encode and decode cleartext and ciphertext
- Discuss how encryption enables secure transmission of sensitive data
- Explain and compare symmetric and asymmetric cryptography
- Describe the role of public key infrastructure and key management

Communication and Network Security

This course covers topics related to communications and network security. It begins with a lesson in the different types of networks and different transmission technologies. It also covers the two main models that govern how networks work: the OSI model and the TCP/IP model, as well as their related layers. The course includes a detailed discussion of the many protocols that allow networks and network devices to communicate with one another and includes a discussion of firewalls and wireless networks. This course is designed for IT professionals and other adult learners who are interested in gaining an introduction to information technology security.

Learning Outcomes

- Discuss the general concepts that enable networking and its role in information technology
- Compare the different types of networks, including LANs, WANs, and MANs, as well as the Internet, intranets, and extranets
- Explain what the Open Systems Interconnection (OSI) Reference Model is and identify its seven layers
- Contrast the OSI model with the TCP/IP Model
- Identify common protocols and differentiate between network, routing, and data link protocols
- Describe the functions of common networking devices, including bridges, routers, hubs, repeaters, switches, and firewalls
- Discuss how wireless networks work and the technology that enables them
- Identify common network attacks and how they can be prevented

Identity and Access Management

This course introduces students to the principles of access controls, beginning with the central modes of information security and continuing through various attacks and defenses. The course presents different kinds of authentication techniques, how they work, and how they are distinguished from each other. This course requires some basic understanding of IT concepts.

Learning Outcomes

- Understand the key principles and terminology of information access control
- Discuss different types of identification and authorization techniques
- Describe common access control models and mechanisms
- Identify common access control attacks and countermeasures

Security Assessment and Testing

This course covers security assessment and testing, focusing on potential disruptions affecting organizations and how they can be addressed with assessments and plans. Students will have the opportunity to practice how to assess the impact of disasters that may arise, as well as to develop their versions of these plans. This course requires a basic understanding of IT concepts.

Learning Outcomes

- Relate the many potential disasters and disruptions that can impact organizations and their information systems
- Describe the steps required in conducting a business impact assessment
- Explain the difference between a business continuity plan and a disaster recovery plan
- Discuss different recovery strategies and how they fit into disaster recovery planning
- Understand the business continuity organization and its responsibilities
- Prepare a business continuity and disaster recovery plan
- Discuss how organizations test their BCPs and DRPs, and perform different exercises to prepare for disruptions

Security Operations

This course contains a detailed overview of security operations, including administrative controls, trusted recovery, and change and incident management. It establishes a foundation in auditing, monitoring, and detection in information security and requires a basic understanding of IT concepts.

Credits

- 0.5IACET CEUs
- 5HRCI Credits
- 5SHRM PDCs
- 5ATD CI Credits
- 5PMI PDUs:
    - 2.5Ways of Working PDUs
    - 1Power Skills PDUs
    - 1.5Business Acumen PDUs

Learning Outcomes

- Understand the role of security operations and discuss its key themes
- Discuss several administrative controls and explain how they can improve information security
- Compare different security controls and explain how they work
- Identify trusted recovery techniques
- Relate the steps required in effective incident management and response
- Discuss the role of auditing, monitoring, and detection in information security
- Describe the steps involved in a digital forensics' investigation

Software Development Security

This course covers software development security while focusing on the systems development life cycle, operating systems, and their environments. Additional topics include the role of various databases in security and how to recognize and guard against attacks on software. Students will have the opportunity to apply application security controls. This course requires a basic understanding of IT concepts.

Learning Outcomes

- Discuss the role of security in software development
- Explain the systems development life cycle and compare its eight stages
- Understand what the operating system is and how it works
- Describe different application and operating environments
- Discuss the role of databases in information security and identify different database types
- Apply several application security controls
- Recognize several software-based attacks and describe methods to guard against them

Credits

- 4 IACET CEUs
- 30 SHRM PDCs
- 30 PMI PDUs:
  - 16.5 Ways of Working PDUs
  - 4 Power Skills PDUs
  - 9.5 Business Acumen PDUs
- 30 HRCI Credits
- 40 ATD CI Credits

Accreditations