SAFEGUARD YOUR ORGANIZATION FROM CRITICAL VULNERABILITIES WITH A

CYBERSECURITY BUNDLE

PLACE ORGANIZATION NAME HERE

WHY EARN A CERTIFICATE IN REAL-WORLD CYBERSECURITY SCENARIOS?

The process of identifying and mitigating cyber threats is just one aspect of cybersecurity. As technology advances, cyberattacks are only going to become more frequent and harder to identify. Cybersecurity professionals must continuously refine and enhance their skills to stay ahead of these threats. One of the most effective training methods is exposure to challenges that cybersecurity professionals currently face.

WHAT WILL I LEARN?

Completing our online certificate in real-world cybersecurity scenarios prepares you to:

- Describe the role of policies, procedures, standards, and guidelines in information security
- Discuss ethical, regulatory, and privacy issues as they relate to information security
- Identify common network attacks and information security risks and how they can be prevented
- Explain the software development life cycle and compare its eight stages
- Understand how cryptography works and its role in information security
- Discuss the foundational concepts of security governance
- Describe common access control models, mechanisms, and identification methods
- Evaluate different security controls such as firewalls, antimalware, and patch management
- Analyze real-world scenarios and make appropriate recommendations to address and improve an organization's cybersecurity

For more information and a complete list of courses, visit:

Place Website URL Here

CAREER PATHS

The U.S. Bureau of Labor Statistics (BLS) expects that overall employment of cybersecurity professionals, such as information security analysts, is projected to grow 33% from 2023 to 2033, much faster than the average for all occupations. About 17,000 openings are projected each year, on average, over the decade.

Common career paths or growth opportunities in cybersecurity include:

Cybersecurity Professional

Cybersecurity professionals protect an organization's data, technology, and other assets from cyberattacks. These professionals often act as the first line of defense against viruses, malicious software, unauthorized users, and natural disasters. Although their responsibilities can vary depending on the needs of the organization, they are often tasked with monitoring network traffic, researching new security technologies, and installing and administering security protocols and solutions.

Information Security Analyst

Information security analysts plan and implement security measures to protect an organization's computer networks and systems. They will likely be involved in developing security standards and best practices for their organizations, as well as recommend security enhancements to management. As organizations focus on enhancing their cybersecurity, they will need these analysts to secure new technologies and procedures from outside threats and hacks.

Information System Security Officer

Information System Security Officers plan, implement, upgrade, and monitor an organization's security measures to protect their data networks. Some of their primary responsibilities include assessing system vulnerabilities for security risks, proposing and implementing risk mitigation strategies, and responding to computer security threats, breaches, and viruses.

The Certificate in Real-World Cybersecurity Scenarios is available 100% online.

The courses included in this certificate carry:

HRCI Credits | PMI PDUs | IACET CEUs | ATD CI Credits | SHRM PDCs

For more information and a complete list of courses, visit:

Place Website URL Here