UNIVERSITY OF MIAMI

Cybersecurity Industry Online Certificate Course (Overview)

With more than 22 billion connected devices expected by 2020, technology has become so deeply integrated with our lives that we often depend on it for our very livelihood. As technology continues to advance, so too do cyber threats. In fact, it's predicted that by 2021, cybercrime will cost the world more than $6 trillion. It is the fastest growing crime in the US, and as it grows, the attacks increase in size and sophistication.

With this increase in cybercrime showing no signs of stopping, people in every industry have been forced to react. From central governments to multinational corporations to small businesses, organizations are desperate to hire qualified cybersecurity personnel. Today, the cybersecurity workforce consists of more than 2.8 million professionals, but another 4.07 billion trained professionals are needed to close the skills gap and satisfy the urgent need for cybersecurity personnel.

Incident Response and Decision Making (4.5 Hours)

This course aims to develop the student's foundational knowledge of cybersecurity, illustrating incident response and decision-making skills that will help them make informed decisions before, during, and after a cyber event.

Students will gain a comprehensive incident-response skill set, from risk management to prevention to decision-making during the peak of an attack. They will also learn the incident response process that every cybersecurity professional uses to assess an event, analyze the data, make the right decision, and take action.

Organizations depend on their cybersecurity personnel to prepare for cyberattacks by constantly monitoring their systems for vulnerabilities, having an action plan to respond to incidents, and being able to make sound decisions during the critical moments of an attack.

Learning Outcomes & Objectives:

Upon completing this course, students will be able to:

- Understand the risks presented by cyber incidents to organizations
- Present the basics of cyber hygiene as a preventative measure
- Explain some of the ways to mitigate the effects of cyber incidents
- Initiate and manage the incident response process
- Make informed decisions for cybersecurity incident prevention and mitigation

Benefits:

- Quickly and accurately identify vulnerabilities, threats, and risks to an organization by analyzing relevant data
- Efficiently respond to incidents, eliminate vulnerabilities, and recover any breached data
- Industry insight that managers and leaders must acquire in order to collaborate with cybersecurity teams and on cross-departmental projects

Contents:

Module 1: What is Cybersecurity? – 1.5 Hours

• Overview

• Threats and vulnerabilities

• Risk management

• Case studies

Module 2: Cyber Hygiene - 1 Hours

• Personal security

• IT security frameworks

• Hardening systems

• Hardening networks

• Hardening humans

• Case studies and exercises

Module 3: Incident Response - 2 Hours

• Defining an incident

• Digital forensics & incident response: The big picture

• Incident response operations

• Incident response methodologies, regulations, and standards

• Incident response technologies

• Biases in human decision making

• Case studies and exercises