Master of Science in Cybersecurity

Syllabus for CYB740 Incident Response and Remediation

NOTE: This syllabus document contains the basic information of this course. The most current syllabus is available in the full course.

Course Description

Addresses how to set up an incident response system in an organization and the phases of an IR: Preparation, Identification, Notification, Containment, and Eradication of the threat actors, and Recovery and Reporting to prevent future incidents. Students will learn about the use of IDS and forensics, dealing with false alarms and the remediation process to minimize business impact, plan business continuity, and work with law enforcement, auditors, insurance, and compliance.

Prerequisite(s)

CYB 700, 703, 705, 707, 715, 720

Program Outcomes

This course addresses the following competencies and program outcomes of the Masters of Science in Cybersecurity:

- Program Outcome 3: Design, evaluate, and test systems including networks, computers, and hardware for security requirements
- Program Outcome 7: Conduct security risk management assessments
- Program Outcome 8: Develop and implement threat management framework
- Program Outcome 9: Evaluate and create security policies and processes for an organization and apply appropriate security frameworks
- Program Outcome 11: Assess trends in computer criminology and social behaviors related to technology use including physical security
- Program Outcome 12: Engage in ethical decision-making and apply ethical principles to cybersecurity
- Program Outcome 13: Engage in professional collaboration and communication with technical and nontechnical stakeholders on issues related to security
- Program outcome 14: Develop and implement an incident response strategy
- Program outcome 16: Interpret legal implications of security incidents and conduct investigations using industry best practices

Course Outcomes

Upon completing this course, you will be able to do the following:

1. Describe steps in the response to a cybersecurity incident
2. Build an incident response team within an organization
3. Plan for actions to minimize impacts of incidents on business
4. Understand how to work with law enforcement and external organizations after an incident

Course Components

Quizzes

Every topic will include a quiz that covers foundational terminology and concepts.

Discussions

The purpose of lesson discussions is to engage in critical reflection and dialogue with classmates regarding course content.

Major Project: Industry Incident Response Plans

Throughout the semester, you will be working toward constructing Incident Response Plans for different industry scenarios.

Grading

The following grading scale will be used to evaluate all course requirements and to determine your final grade:

Grade	Percentage Range
A	>94%
A-	>90%
B+	>87.5%
B	>85%
B-	>80%
C+	>77.5%
C	>70%
C-	>65%
F	<65%

Assignment	Points
Quizzes (10 best of 11 @ 25 pts.)	250
Discussion (6 @ 20 pts.)	120
Assignment 1: Incident Response Preparation	30
Assignment 2: Contingency Planning - Business Continuity	30
Assignment 3: IR Plan - Analysis	30
Assignment 4: Using Detection Tools in Incident Response	30
Assignment 5: Incident Remediation	30
Final IR Plan	230
Total Points	**750**