Enterprise Incidence Response

ISM 441

Southwestern College Professional Studies

COURSE SYLLABUS

I. Course Catalog Description

Learners develop the knowledge and skills necessary to create an information security incident plan, lead an information security incident response, and conduct an information security incident investigation. Topics include the plan components, security incident response methods, and the investigation process. *Prerequisite*: SMGT320.

II. Required and Supplementary Instructional Materials

Whitman, M. E., Mattord, H. J., & Green, A. (2014). *Principles of incident response and disaster recovery* (2nd ed.). Boston: Cengage Learning. Print ISBN: 9781111138059. This ebook is included in the course fees for this class. No additional book purchase is necessary.

III. Learning Outcomes

Learning outcomes describe the knowledge, skills, values, and attitudes that learners gain as the result of a particular learning experience. Southwestern College Professional Studies has learning outcomes specific to each course and each undergraduate and graduate program of study, as well as institution-wide outcomes related to the mission and vision of the college. Outcomes can help learners and instructors focus on the big picture of the learning experience and can help inform potential employers about a graduate's knowledge and skills.

Upon successfully completing this course, the learner will be able to:

1. Categorize circumstances that qualify as an information security incident.
2. Evaluate the incident response and investigatory requirements for variant information security incident scenarios.
3. Critique best practices for executing an incident response and conducting an incident investigation for variant incident scenarios.
4. Recommend a detailed incidence response and investigation action plan for variant incident scenarios.
5. Propose a comprehensive information security incident plan to meet an organization's information security requirements.

At the end of the course, learners may vary in their ability to achieve these outcomes. You are more likely to achieve these outcomes only if you attend class and/or online activities as required by the syllabus, complete the requirements for all assignments to the best of your ability, participate actively in class activities and group work as directed, and study diligently for exams.

IV. Course Policies

Students are expected to read and abide by the course policies located in the instructor-specific syllabus in the blackboard course.

V. Course Requirements:

Requirements	Number of Assignments	Points Possible	Percent of Grade
Discussions	12	240	20%
Exercises	3	150	15%
Essays	2	70	10%
Professional Skills	6	240	25%
Mastery Assignments	3	300	30%

Requirements	Number of Assignments	Points Possible	Percent of Grade
Total Points	**26**	**1000**	**100%**

VI. Course at a Glance:

Unit	Reading & Preparation Activities	Graded Work Due
1	• *Principles of Incident Response and Disaster Recovery*: Chapters 1–2 • "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It" by Michael Riley et al. • "Information Security & Risk Management," an interview with information security expert Ian Mann	Discussion 1 Discussion 2 Exercises Professional Skills: Memo
2	• *Principles of Incident Response and Disaster Recovery*: Chapters 3–4 • "Incident Response Team Best Practices," an interview with Lenny Zeltser • "Computer Security Incident Handling Guide" by the National Institute of Standards and Technology	Discussion 1 Discussion 2 Essay Professional Skills: Memo
3	• *Principles of Incident Response and Disaster Recovery*: Chapters 5–6 • "Intrusion Detection Best Practices" by AlienVault • "Startup to Facebook: Want to See the Security Flaw We Found? Come to Tel Aviv & Get It Yourself" by Richard Reilly	Discussion 1 Discussion 2 Exercises Professional Skills: Memo Mastery Assignment
4	• *Principles of Incident Response and Disaster Recovery*: Chapters 7–8 • "The Disclosure Debate: When Should Companies Reveal Cyber Attacks?" by Matt Egan • "What Is Electronic Discovery?" by Bill Dean	Discussion 1 Discussion 2 Exercise Professional Skills: Cost/Benefit Comparison Mastery Assignment
5	• *Principles of Incident Response and Disaster Recovery*: Chapters 9–10 • "FBI: Contract Worker Set Fire at FAA Center" by Peter Nickeas, Jon Hilkevitch, & Tony Briscoe • "AT&T's Incredible Disaster Recovery Team: A Video Tour" by Michael Fisher	Discussion 1 Discussion 2 Essay Mastery Assignment
6	• *Principles of Incident Response and Disaster Recovery*: Chapters 11–12 • "Business Continuity Related Infographics" by the Business Continuity Institute • "Business Continuity Management—The Time Is Now" by the Business Continuity Institute	Discussion 1 Discussion 2 Professional Skills: Presentation Professional Skills: Memo

VII. Other Policies and Requirements

Follow this link to the Southwestern College Professional Studies Standard Syllabus in Blackboard. You may be required to log in.