CYBR C170: CYBERCRIME AND CSIRT COORDINATION

Item	Value
Curriculum Committee Approval Date	10/27/2023
Top Code	070800 - Computer Infrastructure and Support
Units	3 Total Units
Hours	68 Total Hours (Lecture Hours 54; Lab Hours 14)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

Students will explore an introduction to laws relevant to cybercrime and the roles of the Cyber Security Incident Response Team (CSIRT). Topics covered include international, federal, and state laws relevant to cybercrime, an overview of the U.S. court system and jurisdictions, CSIRT coordination within the team and with stakeholders internal to the organization, ethics pertaining to cyber professionals, project management, technical writing, countermeasures, and compliance. This course is intended for students with an interest in cyber defense for private organizations or government law enforcement. Careers and emerging trends in the field of cybersecurity will be evaluated. ADVISORY: CYBR C150. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Demonstrate an understanding of the typical roles and interactions of a Cyber Security Incident Response Team (CSIRT).
2. Apply diverse viewpoints to ethical dilemmas in the cybersecurity field and recommend appropriate actions.
3. Develop a technical report using appropriate, industry-recognized terminology.

Course Objectives

- 1. Describe the roles of the Cyber Security Incident Response Team (CSIRT) members.
- 2. Describe methods of addressing ethical issues in the field of cybersecurity.
- 3. Describe emerging cybersecurity trends related to cybercrime and incident response teams.
- 4. Describe digital evidence and the purpose of criminal investigations.
- 5. Explain how to think like an adversary.
- 6. Define data preservation techniques and the purpose within the context of investigations.

Lecture Content

Federal and State Laws US Court system / jurisdictions federal state local civil vs. criminal International laws Regulatory Agencies Compliance Relevance to the collection and identification of evidence IR team collaboration Define CSIRT roles IR Team dynamics and interactions with stakeholders Review case studies related to issues of integrity to understand ethical behaviors Project management Court preparation Technical writing Technical style and organization Practice condensing information succinctly without sacrificing content Identify audiences Apply proper style for audience Countermeasures

Lab Content

Students will work with remote lab environments to complete hands-on activities. Case review Simulated case analysis Mock scenario for incident responders Technical writing for cybersecurity

Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)
- Lab (04)
- DE Live Online Lab (04S)
- DE Online Lab (04X)

Instructional Techniques

This course will utilize a combination of lecture, hands-on guided laboratory assignments, classroom/discussion student interactions, problem solving, quizzes, tests, and troubleshooting assignments to achieve the goals and objectives of this course. All instructional methods are consistent across all modalities.

Reading Assignments

Read about and research the role of the CSIRT and its team members. Read about the international, federal, local laws, and industry reglations applicable to organizations.

Writing Assignments

Prepare a preliminary report for upper management on the incident at hand, success or failure in managing the threat, and its impact on the organization.

Out-of-class Assignments

Review cases containing ethical issues and suggest appropriate actions.

Demonstration of Critical Thinking

Students will analyze ethical issues and recommend appropriate actions.

Required Writing, Problem Solving, Skills Demonstration

Skills will be demonstrated through case reviews detailing the role of the CSIRT and its members and procedures followed by the team involving evidence collection.

Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience. Computer service technology: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience.

Textbooks Resources

1. Required Holt, T.; Bossler, A.; Seigfried-Spellar, K. Cybercrime Digital Forensics, 3rd ed. Routledge, 2022 Rationale: -

Other Resources

1. Coastline Library 2. OER - Open Educational Resources