CYBR C227: CYBER-PHYSICAL SECURITY: PROTECTING CRITICAL INFRASTRUCTURE

Item	Value
Curriculum Committee Approval Date	04/24/2020
Top Code	070800 - Computer Infrastructure and Support
Units	3 Total Units
Hours	54 Total Hours (Lecture Hours 54)
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 cyber-physical security using a risk-informed, all-hazards approach to safeguarding critical infrastructure in cyberspace that emphasizes protections for privacy and civil liberties, transparent and accessible security processes, and domestic and international partnerships that further collective action. Topics covered include an analysis of cyber threats and vulnerabilities to understand more fully the interdependency of infrastructure systems nationwide, and that cyber and physical security are interdependent as core aspects of corporate risk management strategies. 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 C225 and CST C230. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Evaluate risk management strategies of critical infrastructure to recommend best practices for ways to prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents.
2. Analyze the interdependency of infrastructure systems nationwide.
3. Develop a technical report using appropriate, industry-recognized terminology.

Course Objectives

- 1. Describe how the Department of Homeland Security coordinates with sector specific agencies, other federal agencies, and private sector partners to share information on and analysis of cyber threats and vulnerabilities.
- 2. Examine the need for cyber-physical security of critical infrastructure.
- 3. Analyze how cyber and physical security are interdependent and must be core aspects of risk management strategies.

Lecture Content

Protecting Critical Infrastructure: Issues in Cyber-Physical Security Cybersecurity Terminology and Frameworks Assessing Cyber Threats and Solutions for Municipalities Cyber Perimeters for Critical Infrastructure A Security Evaluation Cyber Risks in the Marine Transport System Creating a Cybersecurity Culture The Community Cybersecurity Maturity Model Fighting Cyber Crime: A Joint Effort Cybersecurity Challenges Get People Involved in Cyber-Physical Security Cybersecurity, Trust-Building, Trust-Management: Tools for Multi-Agency Cooperation An Analysis of the Nature of Spam as Cybercrime Securing the Automotive Critical Infrastructure

Method(s) of Instruction

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

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 Department of Homeland Security and critical infrastructure agencies. Read about sector-specific agencies, other federal agencies, and private sector partners that share information and analysis of cyber threats and vulnerabilities relating to critical infrastructure.

Writing Assignments

Document best practices for critical infrastructure agencies to take a collective approach to prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents. Document best practices for critical infrastructure agencies to prioritize cyber incidents.

Out-of-class Assignments

Review cases of cyber incidents at critical infrastructure agencies. Summarize case studies that demonstrate working relationships between critical infrastructure agencies and private-sector organizations.

Demonstration of Critical Thinking

Students will analyze critical infrastructure case studies and recommend appropriate actions.

Required Writing, Problem Solving, Skills Demonstration

Skills will be demonstrated through case reviews detailing the roles of multiple critical infrastructure agencies followed by recommendations for best practices in cyber-physical security.

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 Clark, R.; Hakmin, S. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level, 1st ed. New York City: Springer, 2017

Other Resources

1. Coastline Library 2. OER - Open Educational Resources