Course Acronym:	CIS
Course Number:	119
Descriptive Title:	Introduction to Computer Security
Division:	Business
Department:	Computer Information Systems
Course Disciplines:	Computer Information Systems
Catalog Description:	This course introduces students to computer security in a networked environment, and methods to identify and prevent cybercrimes. Types of cybercrimes explored range from alteration of computer software to direct access attacks and data tampering. Topics include security for communication networks, infrastructure security, authentication types, malicious code, intrusion detection, cryptography, and biometrics. Vulnerabilities in cloud computing, mobile platforms, web services, and the Internet of Things is also covered. This course will prepare students to take the CompTIA Security+ Certification exam.
Prerequisite:	Computer Information Systems 13 with a minimum grade of C or equivalent experience
Co-requisite:	
Recommended Preparation:	
Enrollment Limitation:	
Hours Lecture (per week):	2
Hours Laboratory (per week):	3
Outside Study Hours:	4
Total Course Hours:	90
Course Units:	3
Grading Method:	Letter Grade only
Credit Status:	Credit, degree applicable
Transfer CSU:	Yes
Effective Date:	4/18/2016
Transfer UC:	No
Effective Date:	
General Education: ECC	
Term:	
Other:	

CSU GE:	
Term:	
Other:	
IGETC:	
Term:	
Other:	
Student Learning Outcomes:	**SLO #1** Demonstrate the knowledge necessary to create a secure computer environment. **SLO #2** Apply the concepts of cybersecurity and the regulatory standards and compliances to a computer installation. **SLO #3** Define Firewall and intrusion detection and identify the needed countermeasures. **SLO #4** Demonstrate an understanding of the processes and goals of a cyberforensics investigation.
Course Objectives:	1. Identify the various categories of cybercriminals. 2. Compare and contrast the differences between cybercrimes against individuals, organizations, and society at large. 3. Understand the challenges of securing information. 4. Apply knowledge of computer hardware, software, file systems and networks in identifying and resolving computer crime and information security incidents. 5. Understand vulnerability assessment and explain why it is important to a business. 6. Identify software and hardware technologies needed to defend against intrusions from adversaries, malicious actors and malware.
Major Topics:	**I. Introduction to Security (3 hours, lecture)** A. Understand Security B. Challenges of Securing information C. Cybercriminals **II. Network Security (3 hours, lecture)** A. Network Devices and Technology B. Secure Network Administration Principles C. Network Design Elements and Compounds D. Network Protocols **III. Compliance and Operational Security (3 hours, lecture)** A. Risk Analysis B. Risk Mitigation Strategies C. Incident Response Procedures D. Security Awareness and Training E. Business Continuity

F. Environmental Controls
G. Recovery Plans and Procedures

IV. Threats and Vulnerabilities (4 hours, lecture)
A. Malware
B. Social Engineering Attacks
C. Wireless Attacks
D. Application Attacks
E. Mitigation and Deterrent Techniques
F. Penetration Testing

V. Application, Data and Host Security (3 hours, lecture)
A. Application Security
B. Host Security Procedures
C. Importance of Data Security

VI. Access Control and Data Management (3 hours, lecture)
A. Authentication Services
B. Authentication, Authorization and Access Control
C. Account Management

VII. Cryptography (3 hours, lecture)
A. Concepts
B. Tools and Products
C. Public Key Infrastructure
D. Certificate Management
E. Associated Components

VIII. Administer a Secure Network (2 hours, lecture)
A. Common Network Protocols
B. Network Administration Principles

IX. Wireless Network Security (3 hours, lecture)
A. Wireless Attacks
   1. Wireshark
   2. Beacon Frame
B. Vulnerabilities of IEEE Wireless Security
C. Wireless Security Solution

X. Mobile Device Security and Internet of Things (3 hours, lecture)
A. Mobile Device Risk
   1. Bluetooth
   2. Intercept Wireless Data
B. Secure Mobile Device
C. App Security
D. Internet of Things
   1. Privacy
   2. IOT in Business

XI. Cloud Computing (3 hours. lecture)
A. Types of Cloud
B. Cloud Service Models
C. Advantages

D. Disadvantages

XII. Vulnerability Assessment (3 hours, lecture)
A. Vulnerability Scan vs Penetration Test
B. Assessment Techniques
C. Privilege Escalation
1. Zenmap
2. Metasploit
3. Nmap

XIII. Secure Wireless Networking (6 hours, lab)
A. Security Issues
B. Types of Wireless Attacks
C. FTP
D. TCP
E. POP

XIV. Network Devices and Technologies (6 hours, lab)
A. Network Traffic
B. pfSense Firewall
C. Protocols and Default Network Ports
1. Telnet
2. SSH

XV. Incident Response Procedures (6 hours, lab)
A. Compliance
B. Risk Mitigation Strategies
C. Risk Assessment Procedures
D. Netstat
E. Ipconfig

XVI. Network Administration Principles (6 hours, lab)
A. Network Administration Security
B. Mitigation Techniques
C. Deterrent Techniques
D. Password Cracking
E. Web Application Attacks

XVII. Identify and Analyze Network/Host Intrusion (6 hours, lab)
A. Detection System Alerts
B. Discovering Threats
C. Vulnerability Scanning

XVIII. Data Security Using Encryption Software (4 hours, lab)
A. Social Engineering Toolkit
B. Public Key Encryption

XIX. Authentication, Authorization, and Access Control (6 hours, lab)
A. Install Security Controls
B. Configure Security Controls
C. Account Management

XX. Cryptography (4 hours, lab)

	A. Techniques B. Methods **XXI. Wireless Networks (3 hours, lab)** A. Wireshark B. Beacon Frame **XXII. Mobile Security (3 hours, lab)** A. Android Emulator B. Install Security Apps C. Anti-Malware Apps **XXIII. Vulnerability Scanners and Penetration Testing (4 hours, lab)** A. Privilege Escalation B. Zenmap C. Metasploit D. Nmap
Total Lecture Hours:	36
Total Laboratory Hours:	54
Total Hours:	90
Primary Method of Evaluation:	2) Problem solving demonstrations (computational or non-computational)
Typical Assignment Using Primary Method of Evaluation:	Zack is a professor of Computer Science at a University here in Surf City. He got an angry email from the Network Operations Center (NOC) at the University saying that his lab's server was infected with a worm -- the NOC determined this because of a huge spike in Internet traffic which occurred at 4 in the morning. He immediately shut it down and brought it in to be imaged. He doesn't think it was infected, but the University wants independent confirmation before they will put it back online. Zack told you that the machine was just being installed; there were hardly any files on it except for his own account and some student accounts. Create a one-to two-page report that would respond to the following: Was the server compromised? If so, how? If not, what happened? Is it good enough to delete the obvious files? Could the system be Trojaned? What needs to happen before the system is put back into service?
Critical Thinking Assignment 1:	It appears as if a hacker broke in a server at Dempsey Healthcare Systems, stole a protected spreadsheet chock full of patient information, and got caught trying to fence it to an undercover cop via Facebook. They tracked down the accused hacker. He says he got the spreadsheet file "from a friend" but his story does not check out. The feds seized his computer with an outstanding warrant for "Second Degree Music Piracy" but did not find any evidence on it, so if they are going to get him for more than "Possession of Stolen Information," they need reasonable proof that he actually stole the spreadsheet. Finally, Dempsey's Defense wants your professional recommendation as to what they need to do before putting the server back into production. They would each like a one-to two-page "post mortem" report detailing all relevant discoveries, including:

	How you think the server was compromised How you think the attacker accessed any sensitive information What to do to protect their clients from potential identity theft What should be done before returning the system to production
Critical Thinking Assignment 2:	A medium-sized company based in Loxton with an E-government business model has recently begun to notice anomalies in its accounting and product records. It has undertaken an initial check if system log files, and there are a number of suspicious entries and IP addresses with a large amount of data being sent outside the company firewall. They also recently received a number of customer complaints saying that there is often a strange message displayed during order processing, and they are often re-directed to a payment page that does not look legitimate. In a one-to two-page paper describe: How you would approach the following investigation? What additional actions might you recommend?
Other Evaluation Methods:	Laboratory Reports, Multiple Choice, Other Exams, Quizzes
Instructional Methods:	Lab, Lecture, Multimedia presentations, Other (specify)
If other:	
Work Outside of Class:	Problem solving activity, Required reading, Study, Written work (such as essay/composition/report/analysis/research)
If Other:	
Up-To-Date Representative Textbooks:	Mark Ciampa. Security+ Guide to Network Security Fundamentals. 7th ed. Cengage, 2022.
Alternative Textbooks:	Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals, 6th ed., Cengage, 2018.
Required Supplementary Readings:	
Other Required Materials:	USB 2.0 flash drive 8 GB or larger
Requisite:	Prerequisite
Category:	sequential
Requisite course(s): List both prerequisites and corequisites in this box.	Computer Information Systems 13 with a minimum grade of C OR
Requisite and Matching skill(s):Bold the requisite skill. List the	**Demonstrate an understanding of the development and use of information systems in business.**

corresponding course objective under each skill(s).	CIS 13 -Explain the development and use of information systems in business. **Identify the impact of the expanding scope of digital technology including career opportunities, privacy, security, ethics, global relationships, and perceptions of reality.** CIS 13 - Identify and analyze existing and emerging technologies and their impact on organizations and society including computer, communication and information systems, privacy, security, crime, ethics, global relationships, and career opportunities.
Requisite Skill:	equivalent experience
Requisite Skill and Matching Skill(s): Bold the requisite skill(s). If applicable	
Requisite course:	
Requisite and Matching skill(s):Bold the requisite skill. List the corresponding course objective under each skill(s).	
Requisite Skill:	
Requisite Skill and Matching skill(s): Bold the requisite skill. List the corresponding course objective under each skill(s). If applicable	
Enrollment Limitations and Category:	
Enrollment Limitations Impact:	
Course Created by:	Monica Chaban
Date:	10/22/2015
Original Board Approval Date:	04/18/2016
Last Reviewed and/or Revised by:	Richard Perkins
Date:	04/25/2018
Last Board Approval Date:	12/19/2022