CSE 4471 (Approved): Information Security

Course Description

Introduction to security of digital information; threats and attacks; regulations; risk management; attack detection and response; cryptography; forensics; technical training and certifications.

Prior Course Number: CSE 551
Transcript Abbreviation: Info Sec
Grading Plan: Letter Grade
Course Deliveries: Classroom
Course Levels: Undergrad, Graduate
Student Ranks: Junior, Senior
Course Offerings: Autumn, Spring
Flex Scheduled Course: Never
Course Frequency: Every Year
Course Length: 14 Week
Credits: 3.0
Repeatable: No
Time Distribution: 3.0 hr Lec
Expected out-of-class hours per week: 6.0
Graded Component: Lecture
Credit by Examination: No
Admission Condition: No
Off Campus: Never
Campus Locations: Columbus
Prerequisites and Co-requisites: (CSE 2231 and CSE 2321) or CSE 321
Exclusions: Not open to students with credit for CSE 551
Cross-Listings:

The course is required for this unit's degrees, majors, and/or minors: No
The course is a GEC: No
The course is an elective (for this or other units) or is a service course for other units: Yes

Subject/CIP Code: 14.0901
Subsidy Level: Doctoral Course

Programs

Abbreviation	Description
BS CSE	BS Computer Science and Engineering
MS CSE	MS Computer Science and Engineering
PhD CSE	PhD Computer Science and Engineering

Course Goals

Be competent with information security governance, and related legal and regulatory issues
Be competent with understanding external and internal information security threats to an organization
Be competent with information security awareness and a clear understanding of its importance
Be competent with how threats to an organization are discovered, analyzed, and dealt with
Be familiar with a high-level understanding of how information security functions in an organization.
Be familiar with the structure of policies, standards and guidelines

Course Topics

Topic	Lec	Rec	Lab	Cli	IS	Sem	FE	Wor
Information security, roles within an organization	1.5							
Legal, regulatory issues	3.0							
Threats, vulnerabilities, exploits	3.0							
Governance, policy, standards, guidelines	3.0							
Risk management	3.0							
Firewalls, Intrusion Detection, Incident Response, Forensics, Honeypots, VPN, Vulnerability Scanning	6.0							
Cryptography	3.0							
Access Control	1.5							
Physical Security, Personnel, Training, Education, Awareness, Certification...	3.0							
Presentations by the students	9.0							
Overview, wrap-up	3.0							

Representative Assignments

Compare/contrast security policies and standards at several Universities
Create attack trees for various scenarios

Grades

Aspect	Percent
Exam	50%
Survey and Presentations	35%
Homework	15%

Representative Textbooks and Other Course Materials

Title	Author
Principles of Information Security, Thomson/Course Technology, ISBN 0-619-21625-5, Third Edition, 2009.	Michael E. Whitman and Herbert J. Mattord

ABET-EAC Criterion 3 Outcomes

Course Contribution		College Outcome
*	a	An ability to apply knowledge of mathematics, science, and engineering.
*	b	An ability to design and conduct experiments, as well as to analyze and interpret data.
*	c	An ability to design a system, component, or process to meet desired needs.
*	d	An ability to function on multi-disciplinary teams.
*	e	An ability to identify, formulate, and solve engineering problems.
**	f	An understanding of professional and ethical responsibility.
*	g	An ability to communicate effectively.
*	h	The broad education necessary to understand the impact of engineering solutions in a global and societal context.

Course Contribution		College Outcome
*	i	A recognition of the need for, and an ability to engage in life-long learning.
**	j	A knowledge of contemporary issues.
*	k	An ability to use the techniques, skills, and modern engineering tools necessary for engineering practice.

BS CSE Program Outcomes

Course Contribution		Program Outcome
*	a	an ability to apply knowledge of computing, mathematics including discrete mathematics as well as probability and statistics, science, and engineering;
*	b	an ability to design and conduct experiments, as well as to analyze and interpret data;
*	c	an ability to design, implement, and evaluate a software or a software/hardware system, component, or process to meet desired needs within realistic constraints such as memory, runtime efficiency, as well as appropriate constraints related to economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability considerations;
*	d	an ability to function on multi-disciplinary teams;
*	e	an ability to identify, formulate, and solve engineering problems;
**	f	an understanding of professional, ethical, legal, security and social issues and responsibilities;
*	g	an ability to communicate effectively with a range of audiences;
*	h	an ability to analyze the local and global impact of computing on individuals, organizations, and society;
*	i	a recognition of the need for, and an ability to engage in life-long learning and continuing professional development;
**	j	a knowledge of contemporary issues;
*	k	an ability to use the techniques, skills, and modern engineering tools necessary for practice as a CSE professional;
*	l	an ability to analyze a problem, and identify and define the computing requirements appropriate to its solution;
*	m	an ability to apply mathematical foundations, algorithmic principles, and computer science theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices;
*	n	an ability to apply design and development principles in the construction of software systems of varying complexity.

Additional Notes or Comments

`Draft, need to especially review the ABET-EC criteria, fix the pre-reqs`

Prepared by: Bruce Weide