Saint Leo University

COM 416
Introduction to Information Security

Course Description:
The advent of global networks has provided communication capabilities for businesses and individuals unparalleled in the history of the world. Attacks on the system that deny service, destroy systems, and purloin information through the use of worms, viruses, and other criminal attacks make it imperative that information security be a significant part of any business plan and that individuals working in that or allied fields become knowledgeable in the principles of information security. This course provides an introduction to the field of information security that lays a necessary foundation for later courses.

Prerequisite: COM203

Textbooks:
Whitman, M. E. & Mattord, H. J. (2018). *Principles of information security (*6th ed.). Boston, MA: Cengage. ISBN-13: 9781337750714 or the Cengage unlimited access.

(Note: Access to MindTap is only needed for the ebook).

Course Objectives:
The student will be able to:

1. Explain the key terms, essential concepts, and origins of the field of information security.
2. Explain the need for security and the legal, ethical, and professional issues in information security.
3. Explain the process involved in performing a security analysis including identifying, assessing, and controlling risk.
4. Explain the logical design of the accepted security models to the physical design and frameworks including business practices and standards, security policy, technologies employable, planning for information security, inclusion of information security in the systems development life cycle, cryptography utilized, and the physical security employed.
5. Explain the implementation of an information security system including outsourcing, change management, and personnel management.
6. Explain the establishment of an ongoing program for maintaining and evaluating an information security system including risk analysis, risk evaluation, and risk measurement.
7. VALUES OUTCOME: Achieve success in information security, a high degree of integrity and respect for privacy is required. It is necessary for the security analyst to be discrete and not to exploit the discovered vulnerabilities of an organization. These core values are inherent to this course and frequently come up in discussions.

Integrity: The commitment of Saint Leo University to excellence demands that its members live its mission and deliver on its promise. The faculty, staff, and students pledge to be honest, just, and consistent in word and deed.

Evaluation:

Your grade in this course will be determined by a number of factors. Grading will be evaluated in the following manner:

In determining the final grade, the following weights will apply:

Assessment	**Percentage**
Midterm Exam	15%
Final Exam	20%
Assignments (8)	40%
Discussions (8)	15%
Project Paper	10%
TOTAL	**100%**

Final letter grade will be based on the following scale:

A	94-100
A-	90-93
B+	87-89
B	84-86
B-	80-83
C+	77-79
C	74-76
C-	70-73
D+	67-69
D	60-66
F	0-59

Course Schedule:

Module 1 Introduction to Information Security

Objectives When you complete this module, you should be able to:

- Define information security.
- Explain the history of computer security and how it evolved into information security.
- Explain key terms and critical concepts of information security as presented in this chapter.
- Describe the critical characteristics of information.
- Discuss the phases of the security systems development life cycle.
- Describe the roles of professionals involved in information security within an organization.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an introduction to the class	Thursday 11:59 PM EST/EDT
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Assignment M1	Sunday 11:59 PM EST/EDT

Module 2 The Need for Securing Information Systems

Objectives When you complete this module, you should be able to:

- Explain that organizations have a business need for information security.
- Explain that a successful information security program is the responsibility of both an organization's general management and IT management.
- Identify the threats posed to information security and the more common attacks associated with those threats.
- Differentiate threats to the information within systems from attacks against the information within systems.
- Describe the issues facing software developers, as well as the most common errors made by developers, and explain how software development programs can create software that is more secure and reliable.
- Differentiate between laws and ethics, identify major national laws that relate to the practice of information security, and describe the role of culture as it applies to ethics in information security.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Assignment M2	Sunday 11:59 PM EST/EDT

Module 3 Planning for Security

Objectives When you complete this module, you should be able to:

- Discuss management's role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines.
- Describe what an information security blueprint is, what its major components are, and how it is used to support the information security program.
- Discuss how an organization institutionalizes its policies, standards, and practices using education, training, and awareness programs.
- Explain what contingency planning is and how incident response planning, disaster recovery planning, and business continuity plans are related to contingency planning.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Begin working on Project Paper	
Submit Assignment M3	Sunday 11:59 PM EST/EDT

Module 4 Risk Management

Objectives When you complete this module, you should be able to:

- Define risk management, risk identification, and risk control and explain how risk is identified and assessed.
- Assess risk based on probability of occurrence and impact on an organization.
- Describe the fundamental aspects of documenting risk through the creation of a risk assessment and the risk mitigation strategy options for controlling risks.
- Identify the categories that can be used to classify controls.

- Recognize the conceptual frameworks that exist for evaluating risk controls and be able to formulate a cost benefit analysis.
- Describe how to maintain and perpetuate risk controls.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Assignment M4	Sunday 11:59 PM EST/EDT
Complete Midterm Exam	Sunday 11:59 PM EST/EDT

Module 5 Security Technology

Objectives When you complete this module, you should be able to:

- Explain the role of physical design in the implementation of a comprehensive security program.
- Describe firewall technology and the various approaches to firewall implementation.
- Identify the various approaches to remote and dial-up access protection and the technology involved that which enables the use of virtual private networks.
- Identify and describe the categories and operating models of intrusion detection systems including honey pots, honey nets, and padded cell systems.
- List and define the major categories of scanning and analysis tools, and describe the specific tools used within each of these categories.
- Explain the various methods of access control, including the use of biometric access mechanisms.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Assignment M5	Sunday 11:59 PM EST/EDT

Module 6 Cryptography and Physical Security

Objectives When you complete this module, you should be able to:

- Describe the most significant events and discoveries in the history of cryptology and explain the basic principles of cryptography.
- Describe the operating principles of the most popular tools in the area of cryptography and the major protocols used for secure communications.
- Discuss the nature and execution of the dominant methods of attack used against cryptosystems.
- Discuss the relationship between threats to information security and physical security
- Describe the key physical security considerations including fire control and surveillance systems.
- Identify critical physical environment considerations for computing facilities, including uninterruptible power supplies.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Assignment M6	Sunday 11:59 PM EST/EDT

Module 7 Implementing Information Security

Objectives When you complete this module, you should be able to:

- Explain how an organization's information security blueprint becomes a project plan and the many organizational considerations that a project plan must address.
- Demonstrate the significance of the project manager's role in the success of an information security project.
- Describe technical strategies and models for implementing a project plan.
- Identify the nontechnical problems that organizations face in times of rapid change.
- Explain the issues and concerns related to staffing the information security function
- Describe the special requirements needed to ensure the privacy of personnel data

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT

Submit Assignment M7	Sunday 11:59 PM EST/EDT
Submit Project Paper using the Chalk and Wire Link	Sunday 11:59 PM EST/EDT

Module 8 Information Security Maintenance

Objectives When you complete this module, you should be able to:

- Explain the need for ongoing maintenance of the information security program and the recommended security management models.
- Define a model for a full maintenance program and identify the key factors involved in monitoring the external and internal environment.
- Describe how planning, risk assessment, vulnerability assessment, and remediation tie into information security maintenance.
- Explain how to build readiness and review procedures in information security maintenance.
- Define digital forensics, and describe the management of the digital forensics function
- Describe the process of acquiring, analyzing, and maintaining potential evidentiary material.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Assignment M8	Sunday 11:59 PM EST/EDT
Complete Final Exam	Sunday 11:59 PM EST/EDT

Project Paper Instructions:

Submit the Project Report to **Chalk and Wire** using the link located in the Module 7 folder. Students who do not submit the assignment to Chalk and Wire will receive a zero. This is a key program assessment; the results are used to ensure students are meeting program goals. Video and PDF instructions can be found on the course home page. PDF instructions are also located in the Start Here folder.

Purpose

This project provides you an opportunity to analyze risks, threats, and vulnerabilities and apply countermeasures in the information systems environment.

Introduction

Contemporary organizations collect, store, and transmit a tremendous amount of highly sensitive data. Despite the many benefits that information technology offers, these systems are not completely secure. Proper controls must be put in place to mitigate security risks and protect vital business information.

Scenario

Fullsoft, Inc. is a software development company based in New York City. Fullsoft's software product development code is kept confidential in an effort to safeguard the company's competitive advantage in the marketplace. Fullsoft recently experienced a malware attack; as a result, proprietary information seems to have been leaked. The company is now in the process of recovering from this breach.

You are a security professional who reports to Fullsoft's infrastructure operations team. The Chief Technology Officer asks you and your colleagues to participate in a team meeting to discuss the incident and its potential impact on the company.

Tasks

Prepare for the meeting by deliberating on the following questions:

- How would you assess the risks, threats, and/or vulnerabilities that may have allowed this incident to occur, or could allow a similar incident to occur in the future?
- What insights about risks, threats, and/or vulnerabilities can you glean from reports of similar incidents that have occurred in other organizations?
- What potential outcomes should the company anticipate as a result of the malware attack and possible exposure of intellectual property?
- Which countermeasures would you recommend the company implement to detect current vulnerabilities, respond to the effects of this and other successful attacks, and prevent future incidents?

Write an outline of key points (related the questions above) that the team should discuss at the meeting.

As a reminder, you may use the book for this course and the Internet to conduct research. You are encouraged to respond creatively, but you must cite credible sources to support your work.

Your Project should be submitted in the following format and style:

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Citation Style: APA format, see link https://owl.english.purdue.edu/owl/resource/560/02/
- Length: 5–6 pages double space.
- Due at the end of Module 7.
- Submit to Chalk and Wire

Self-Assessment Checklist

- I have created an outline that describes key points the team should discuss at the meeting. My outline explains how to assess potential risks, threats, and/or vulnerabilities; describes potential outcomes of a malware attack and exposure of confidential information; and recommends countermeasures the company should implement.
- I have conducted adequate independent research for this part of the project.