

Seattle Pacific University
School of Business and Economics

ISM 6331 Information Systems Security
3 Graduate Credits
Winter 2011

Instructor: Gerhard Steinke, Ph.D.
Office: McKenna Hall 203
Office Hours: Mondays and Wednesdays: 1:15 – 3:00 p.m., 5:15 – 6:00 p.m., and by appointment

Email: gsteinke@spu.edu
Phone: (206) 281 - 2377
Fax: (206) 281 – 2733

Classroom: McKenna Hall Conference Room
Class Time: Mondays, 6:00 – 8:50 p.m., Jan. 10 – March 14, 2011.

Textbook: Whitman, Michael and Mattord, Herbert, Principles of Information Security, 4th edition, Course Technology, 2012.

Popular Reading: Charlene Li and Josh Bernoff, Groundswell – Winning in a World Transformed by Social Technologies, Harvard Business Review Press, 2008.

Catalog Description:

“Develops an understanding of information systems security issues. Addresses policy creation, risk evaluation and implementation of security measures in organizations. Examines privacy and ethical issues and legal requirements.” SPU Graduate Catalog

Course Overview

With the move from isolated mainframe to distributed servers and global networks, vast data and information resources are accessible from remote locations. The security of many of these systems and data is vital. Information systems professionals should have an understanding of security concepts, risks, issues and processes to make systems and information more secure. They should also be able to understand management challenges ranging from developing a security policy and risk management, to examining ethical, privacy and legal security requirements.

Course Objectives

MS-ISM students have the following learning objectives. They will demonstrate mastery of the knowledge and skills necessary to be able to:

- Provide values based leadership in the planning, development, and management of information systems
- Effectively integrate information systems with business, strategies, processes and decision-making
- Evaluate the effects of information systems on organizations and personnel
- Assist in managing the organizational transitions brought about by information systems

The objective of this course is to provide students with a deeper understanding of the components and issues in the creation, implementation and management of more secure information systems. There are aspects that fit under all of the above four learning objectives

Specific learning objectives for this course are:

- Understand information security terms, components and measures.
- Be able to develop and implement security policies and processes.
- Plan the steps in managing risk and evaluating information security in an organization.
- Analyze the ethical, legal and privacy concerns related to information security.
- Be acquainted with security publications and internet resources.
- Improve oral and written business communication skills.

Methodology

The course objectives will be achieved through your reading of the text and participation in class, as well as doing the assignments. I expect you to read the related readings before class, so that we have a basis for the discussion and application of the evening's topic. The variety of backgrounds and experiences that you bring to the class will enrich us all. We will have a number of great guest speakers in this class.

Blackboard

We will use Blackboard as a communication vehicle, for me to share information with you (schedule changes, PowerPoint presentations, etc.) as well as for you to share information with others in the class.

Grade Distribution

The course will be graded on a straight percentage scale. Good work will earn a "B" grade. Work "above and beyond" will earn an "A" grade.

A	>95%	C+	>77%
A-	>90%	C	>74%
B+	>87%	C-	>70%
B	>84%	D	>60%
B-	>80%	E	<=60%

Grading

Research Report / Presentation	200	points
Security Assessment	200	
Product Demos	200	
Security Resource Reviews	100	
Final Exam	200	
Class Participation	100	
	=====	
Total Points	1000	

Assignments:

Security Research Report / Presentation (200 points)

Your manager has asked you to research a security-related issue/topic. Make a presentation (15 minutes) and provide us with a written report (approximately 3000 words).

- By January 24: Choose a topic. Sign-up for a presentation date.
- By January 31: Provide me with an outline of the topic and your references (at least 5).

Sample topics: Digital signatures, PKI, wireless security, SQL security, information warfare, VPN, cookies,...

Security Assessment (200 points)

In groups of two, I would like you to perform a security assessment of an organization's information system. Create a report describing their security efforts along with your evaluation and a plan for implementing your recommendations. The report will be about 3000 words with a brief oral executive summary shared with the class. I will provide you with a template listing the types of questions you might ask.

Security Product/Tool Demos (200 points)

Choose two security products. The goal is to make a case to your management to purchase these products to improve the security of the organization's information system. Provide a 700 word analysis and evaluation for each of the products, preferably with demos, including cost, competing products, installation/adoption process, etc. for each security tool/product.

Security Resource Reviews (100 points)

I would like you to review and evaluate 2 security resources. Post a brief review and evaluation (~100 words) on Blackboard. Respond to postings by other students. The resources could be books, periodicals, websites, or you could interview someone who has "security" as a part of their job description.

Final Exam (200 points)

During the final exam you will be asked to respond to several cases.

Class Participation (100 points)

Class contribution is an important part of your learning and evaluation. Students are expected to attend all classes and contribute to the discussion.

Academic Honesty

Academic dishonesty will not be tolerated in any form. Individual assignments must be solely your work and team assignments must be solely the work of your team. Quotes must be footnoted and sources referenced (including WWW references).

Course Evaluation

It is my expectation that you will participate in an online evaluation of this course in a thoughtful and constructive manner. The evaluation data is used to make improvements in the course, and your feedback is considered when selecting textbooks, designing teaching methods and preparing assignments. Courses are evaluated using the Banner Course Evaluation System. All answers are completely confidential - your name is not stored with your answers in any way. In addition, your instructor(s) will not see any results of the evaluation until after final grades are submitted to the University.

Tentative Course Outline

Date	Topic	Text	Popular Reading
Jan. 10	Introduction to IS security, security threats	1, 2	
Jan. 17	Forensics – Guest Presenter – Gordon Mitchell Legal, Ethical Issues – Share your analysis of some IS/IT law with the class.	3	1-2
Jan. 24	Security Assessments, Risk Management – Guest Presenter – Tom Schauer Security Policy and Procedures – share your analysis of a security policy with the class.	4, 5	3-4
Jan. 31	Physical Security Encryption	8, 9	5-6
Feb. 7	Disaster Recovery Planning, Outsourcing Security Email, IM, Spam, Phishing, Social Engineering		7-8
Feb. 14	Network Security, Wireless Security, Intrusion Detection, Penetration Testing, Security Presentations	6,7	9-10
Feb. 21	Security Presentations		11-12
Feb. 28	ISACA/ISA panel – Jack Champlain et.al. Security Presentations	11	
March 7	Security Presentations		
March 14	Final Exam		