

# **Syllabus for IFSM430 (Information Systems and Security)**

## **Course Description**

**Prerequisite:** IFSM 300. A survey covering aspects of establishing and maintaining a practical information security program. The security aspects and implications of databases, telecommunication systems, and software are examined, along with techniques used to assess risks and discover abuses of systems.

## **Course Goals/Objectives**

After completion of this course, you should be able to:

- identify and discuss the fundamental reasons why information systems security is such a critical element in today's business, government, education, and home technology-based environments
- identify and discuss the key information systems security legislative and policy documents that provide guidance in developing an information system security program for an organization
- review and develop the key elements of an information systems security management program
- perform and document a risk-based analysis of information systems security for an organization, to include identification of threats, vulnerabilities, and countermeasures
- develop a security plan to address the results of the risk assessment
- research and report on the key technological solutions to achieving information systems security

## **Course Materials**

Whitman & Mattford Principles of Information Security (2nd ed.). Course Technology-ISBN 0619216255

## **Course Introduction**

The course is based on the security standards as defined by NIST and is presented in the following topic areas:

### **Requirements for Information Systems Security**

We will review incidents that highlight the need for information systems security. These incidents occur at work and at home. They affect our use of information systems and require actions on the part of ourselves and our employers to ensure that systems are available for use. In an age of reliance on the Internet and Internet economy, any

disruptions to Internet systems are costly and may, at times, be life-threatening. It is mandatory that individuals and organizations be aware of and address these issues.

## **Guidance in Developing Information Systems Security Programs**

You will review several key operational documents that will assist you in understanding information systems security. These documents provide the basis for building information systems security programs because they provide guidance that can be used in a specific operational environment. You will also begin to identify and discuss reasons for the development of risk-assessment security plans that provide information assurance and security for organizations.

## **Performing Risk Analyses**

You will follow the NIST guidelines (NIST Special Publications 800-26 and 800-30). Government and industry use this methodology. You may find it interesting that the National Security Agency uses a similar modified method; they call it a Level I Assessment. NSA's Level II Assessment includes monitoring tools; their Level III Assessment includes systems-penetration testing (i.e., hacking) and requires judicial approval.

## **Technology Issues and Solution Tools for Information Systems Security**

This topic deals with many of the technical issues related to information systems security. The list of topics to cover grows on an almost daily basis. You will be provided with relevant URLs for each topic, but we will concentrate on three: viruses, intrusion-detection methods, and the fastest-growing area of interest, biometrics. Each of these topics is worthy of your in-depth study. However, one or several may be of specific interest to you where you work.

## **Ethical and Social Issues Related to Information Systems Security**

The Information Age has brought great benefits. It has also, as we have discovered, raised many issues related to information systems security. In attempting to address those security issues, new and different issues have come to the fore. For each security risk there is a countermeasure. Most of these countermeasures require that controls be put in place, both procedurally and technically. The sum of these controls empowers organizations to monitor an individual's digital world.

## **Grading Criteria**

*Section removed.*

## Academic Policies and Procedures

*Section removed.*

## Project Descriptions

### Suggested projects

- I. **Honeynet Project white papers.** You can access the papers here <http://project.honeynet.org/papers/>

Select one of the papers and write about what you discovered from reading the paper. There are papers here that explain the concept of "Know Your Enemy." The "hacker" community operates a lot like warfare; defending against them requires an understanding of how they operate. This site is a great place to gather that type of information.

- II. **Cryptography.** This paper can be on an algorithm, protocol or a white paper on Cryptography. At a minimum your paper should describe the following: history, security considerations (i.e., has it been hacked, cracked, or is it a concept), where is it being applied, or planned to be applied.

- III. **Digital Millenium Copyright Act (DMCA).** The DMCA has made quite an impact on Internet Security. Your paper should at a minimum contain the following: Introduce the DMCA; When can a program be reverse engineered; IAW the DMCA security considerations with respect to the DMCA, i.e.: how does it affect an organization today? Comments: DMCA fair? Why or why not? How would you change it given the opportunity?

- IV. **Mobile Code.** Mobile Code is something that security professionals have to deal with on a daily basis. Your paper should address the following: Definition of Mobile Code; types of Mobile Code; security considerations with respect to allowing Mobile Code into your internal network; comments: Mobile Code friend or foe?

### Alternate topics:

- V. **Viruses and Worms.** Research the CERT (Computer Emergency Response Team) Web site for the latest reported viruses and worms. Pick any three and discuss what each attack did, what types of systems were affected, and what course of action or remedy was proposed.

**VI. Intrusion-Detection Methods.** Research the various types of intrusion-detection systems that are available to organizations. Discuss the various types and describe the circumstances in which each type should be used. Feel free to use specific examples and products to provide the reader with a complete understanding of the subject.

**VII. Risk Assessment.** Conduct a risk assessment of the information systems in your workplace (or other facility that you may access - i.e., a local library).

### **Requirements For all Papers**

The length of the paper will be determined by the instructor.

#### **1. Writing Quality**

- Grammar, Verb Tenses, Pronoun Use, Spelling, Punctuation, and Writing Competency.
- Remember: spell-check, then proofread. Better yet, have a friend or colleague read it before submitting it. Read it out loud to yourself.
- Remember: *there* is not *their*, *your* is not *you're*, *its* is not *it's*, *too* is not *to* or *two*, *site* is not *cite*, and *who* should be used after an individual, not *that*. For example, "the person WHO made the speech" not "the person THAT made the speech."
- Remember: In a professional paper one does not use contractions (doesn't, don't, etc.) and one does not use the personal *you* or *your*. Use the impersonal as I have in the previous sentence. It is more business-like than saying, "Also in a professional paper you don't use contractions."

#### **2. References**

- Use the APA format for your references.
- The project assumes Internet connectivity or access to outside resources.

#### **3. Word Processor**

- Use Microsoft Word. If you do not have Microsoft Word, Save As a word document.
- Use Page Setup in the Printer to configure it.
- Use 1" margins top, bottom, left and right sides.
- Use Times New Roman, size 12.
- Use double spacing.

- Use appropriate headings and subheadings. Headings and subheadings should be placed at the left margin.
- The first word of each new paragraph should be indented 1" from the. 1" on my Page Setup is 1 tab space.
- For submissions that are longer than 1 (one) page, number each page in the bottom right corner. The cover page should never be numbered.

#### 4. Submissions

Submit the term paper according to instructions given by your instructor (mail/email).

#### 5. Cover Page

Use a cover page. In the center of the page, in this order, double spaced, put:

Your Name; IFSM 430; Name of Topic.

Nothing else needs to be added to the cover page.

### Course Schedule

Week	Readings/Assignments	Due Date
1	chapter 1: Introduction to Information Security (Homework Review Questions pages 35-36, Exercise #5 page 36, due 1st class meeting of the 2nd week)	
2	<b>Project 1: "Know Your Enemy" (Due in Week 4)</b> chapter 2: The Need for Security (Homework Review Questions pages 72-73, Exercise #2 page 73 due the 1st class meeting of the 3rd week)	
3	chapter 3: Legal, Ethical and Professional Issues in Information Security (Homework Review Questions page 112, Exercise #4, and #5 page 112, due the 1st class meeting of the 4th week)	
4	chapter 4: Risk Management: Identifying and Assessing Risk <b>Project 2: "Cryptography" (Due in Week 6)</b> (Homework Review Questions page 148, Exercise #5 page 149, due the 1st class meeting of the 5th week)	
5	chapter 5: Risk Management: Accessing and Controlling Risk (Homework Review Questions pages 184-185, Exercise #5 page 186, due the 1st class meeting of the 6th week)	
6	chapter 6: Blueprint for Security (Homework Review Questions page 231, Exercise #1 page 231 and #4 page 232, due the 1st class meeting of the 7th week)	

7	chapter 7: Planning for Continuity (Homework Review Questions pages 268-269, Case Exercises #1, due the 1st class meeting of the 8th week )	
8	chapter 8: Security Technology (Homework Review Questions pages 317-318, Exercises #3 page 318, Case Exercises #1 page 319, due the 1st class meeting of the 9th week) Appendix: Cryptography pages 323-354	
9	<b>Midterm Exam (chapters 1-8)</b>	
10	<b>Project 3: "DMCA" (Due in Week 12)</b> chapter 9: Physical Security (Homework Review Questions pages 385-386, Case Exercises #2 pages 387-388)	
11	chapter 10: Implementing Security (Homework Review Questions pages 412-413, Case Exercises #2 page 415)	
12	chapter 11: Security and Personnel <b>Project 4: "Mobile Code" (Due in Week 14)</b> (Homework Review Questions pages 446-447, due the 1st class meeting of the 13th week )	
13	chapter 12: Information Security Maintenance (Homework Review Questions page 491, due the 1st class meeting of the 14th week)	
14	Appendix: Cryptography pages 323-354	
15	<b>Final Exam (chapter 1-10)</b>	