Syllabus - MBA 775 - Summer 2018

Instructor Info

Susan Lincke PhD CISA
Associate Professor Computer Science
CISA=Certified Information Systems Auditor

Address:
MOLN 255
University of Wisconsin-Parkside
Kenosha, WI 53141

Email:
lincke@uwp.edu

Phone:
(708) 453-2069

Course Description

While the Internet has been a boon to many businesses, it also poses new threats due to cyber-criminals, who attack from across borders. Students will discuss system vulnerabilities and mitigation strategies and will identify security-related personnel issues and training and education requirements. They will understand the legal and ethical issues surrounding security management and be able to develop and implement security procedures and processes. Topics covered include access control models, information security governance, and information security program assessment and metrics. Coverage on the foundational and technical components of information security is included to reinforce key concepts. Much of the course material is based on security curricula for professional security-related certificates:

Course Objectives

- Understand the issues, technologies and techniques for security and risk management
- Be able to discuss system vulnerabilities and mitigation strategies for information security, network security and physical security
- Develop and implement security procedures and processes to support security policy requirements, including security program measures
- Identify security-related personnel issues, including roles and training and education requirements in managing information security
- Understand the legal and ethical issues surrounding security management and how they affect information security management

Textbook

Textbook: Security Planning: An Applied Approach*. By: Susan Lincke*
Publication: Springer
ISBN: 978-3-319-16026-9

Course Format

Each unit has a commentary that should be read along with the reading from the text book. The text contains examples, additional information (if you are so inclined) and can be used as a reference for the case study. Your understanding of the material is tested in the quizzes. You may take the quizzes multiple times until you get your desired grade. Quiz questions may be randomized. They are due by Thursday evening each week.

An individual discussion enables you to consider how to apply the week's material to your own industry. You get to be a CEO of a new company. Consider how to implement or improve security for your company. (Be sure not to divulge any sensitive information from your current employer.) These are due by Thursday evening each week.

The case study used each week focuses on a doctor's office, which must adhere to HIPAA regulation. Many organizations must adhere to the privacy and security components of the HIPAA regulation, and thus this case is a small (manageable) but good example of security in practice. The weekly case study assignments provide an opportunity to gain hands-on experience in applying the concepts described in the commentaries and the text. The case study comes from a single case study developed as part of an NSF grant intended to help develop information IS security curriculum.

The case study is a group assignment. When doing the case study, you will develop your own answers and submit via a discussion thread by Thursday evening every week. Then the group must reach a reasonable consensus to submit an answer by the following Monday.

Grading Policy

Assignment	% of Grade
Quizzes 7 @ 3.6% each	25%
Individual Discussions 7 @ 3.6% each	25%
Discussions: Case Study 2 @ 5% each	10%
Case Study Group Assignments 7 @ 5.7% each	40%
Total	**100%**

Overall Grading Scale

(La Crosse Students)

Letter	Percentage
A	92 - 100
AB	88 - 91.9
B	82 - 87.9
BC	78 - 81.9
C	70 - 77.9
D	60 - 69.9
F	0 - 59.9

(All other Students)

UW-Oshkosh Letter Grades	UW-Parkside Letter Grades	UWEC/Consortium Letter Grades	Percentage
A	A	A	92 - 100
A -	A -	A -	90 - 91.9
B+	B+	B+	88 - 89.9
B	B	B	82 - 87.9
B -	B -	B -	8 0 - 81.9
C+	C+	C+	78 - 79.9
C	C	C	72 - 77.9
F	C -	C -	70 - 71.9
F	F	D+	68 - 69.9
F	F	D	62 - 67.9

F	F	D -	60 - 61.9
F	F	F	0 - 59.9

Late Work Policy

If you know you will be absent for a due date, plan to submit well in advance. Zero points will be awarded for late discussion work since entering a discussion after it is over is not very beneficial to anyone. Original posts must be made by the original post deadline and follow-up posts must be made by the deadline for follow-up posts. Follow-up posts are not allowed until after the deadline for original posts.

If you have the need for special consideration in regard to an assignment due date, contact me as soon as possible ahead of time and special arrangements may be made - this is subject to my discretion.

Sometimes situations occur that may require an extension on an assignment (death in the family, hospitalization, job responsibility changes). Contact me as soon as you realize the situation is occurring and together we can determine if an extension or an incomplete is advisable or if other action needs to be taken.

Student Expectations

A typical unit will consist of a combination of the following:

1. Reading assignments from the instructor's commentary and the required textbook.
2. A quiz to test for the most important points. (Multiple tries are possible.)
3. Individual discussion in how to apply security to your industry.
4. Discussions you participate in a small group to build your case study answer.
5. An integrated case study that requires you to analyze security issues for a doctor's office.

Expect to spend a minimum of eight to ten hours on the activities assigned in a given unit. The commentary, quiz and individual case study should be completed by Thursday evening, and responses to discussions and the case study completion should occur by the next Monday.

In the individual discussions, you will be asked to generate and participate in the exchange of ideas with the instructors and the other students. You will be designing security related to your industry in the individual discussions. You'll work in small groups for the case study.

If you have questions of a general nature, it is often most useful to post them in the **Raise Your Hand** open forum. Feel free to jump in and help other students if you see a question you can answer before I do and be sure to read other students' posts—your question may already have been asked and answered. Communication that is specific to your situation or is confidential in nature, such as regarding grades, is best done via email.

Instructor Expectations

Most questions can be handled through the Raise your Hand open forum or, if they are of a more sensitive nature, via emails. I will do my utmost to respond to your questions within 24 hours, Monday through Friday. I will likely be online at some time on ***most weekends*** as well, but response time may be longer over a weekend period.
I expect to submit evaluations within 7 days of receiving your finished product and within 7 days after a discussion has closed. When in doubt, do not hesitate to ask! If there are delays for any reason, I will indicate in the news area when you can expect evaluations to appear.

I will make use of the News area on the course homepage regularly to post course related announcements, my thoughts on IS topics, class performance, etc., and other updates and information pertinent to the course.

Academic Honesty Policy

Students are expected to comply with the Academic Honesty requirements specified in the **UW MBA Consortium Student Code of Conduct**.

Additional Information and Resources

Additional information and resources can be accessed via links on the Navigation bar of this course. Specifically:

- For accommodations in accessing web-based materials, refer to the MBA Consortium FAQ: Accessibility Policy.
- For tips and guidance on participating in discussions, refer to the Netiquette policy.
- For resources to help polish your writing skills, refer to Writing Tips.
- For help with accessing reserved library articles (login and password), refer to the Library Guide.

Instructor Bio

Susan Lincke PhD CISA

Hi Everyone!

I welcome you to my course. Since we will not get much of a chance to really meet each other, I would like to introduce myself, as well as describing my background that qualifies me for teaching this course.

I worked at General Electric, MCI Telecommunications, and Motorola in telecommunications before embarking on my teaching career. While in industry, I developed software for networking devices, mobile phones, and quality control; managed telecom projects; and represented Motorola in developing standards for GSM at the European Telecommunications Standards Institute (ETSI). That third part may have been the most fun, since it involved traveling to Europe, participating in standards being developed, and meeting a lot of nice people from all over the world.

After 17 years in industry, I decided to try teaching as a career. I am currently an Associate Professor of Computer Science. I earned my MS and PhD in Computer Science at the Illinois Institute of Technology in Chicago. My PhD research involved simulation and mathematical modeling of wireless networks, with the aim of efficiently distributing traffic across various wireless network types. My current research interests focus on information security and green computing. I am also a Certified Information Systems Auditor (CISA), certified by ISACA.

I received a National Science Foundation grant to develop an Information Security course between 2009-2013. During this grant period, I developed the case study used in my information security courses. The case study involves a Health First doctor's office, to help students design security for a real-life scenario. In the past, students also performed service learning, by designing security for real organizations. As a follow-up to the grant, I authored the text we are using in this course: Security Planning: An Applied Approach. It earned an excellent review from the Association for Computing Machinery, and I hope you enjoy it!

I am married to a retired history teacher and author Gene Salecker, whose specialties are the civil war and WWII in the pacific theater. We live with a cat, rabbit, and fish. I am an avid reader and have lived in Sweden, France and Canada, and traveled to many other countries. I am also interested in gardening, camping and the outdoors. As an animal lover, I am interested in vegetarian cooking, eating and nutrition. To stay calm and happy (most of the time), I meditate daily.

Since I will not get a chance to meet you, I hope you introduce yourself to me! And I hope you enjoy the course and learn a lot from it. If you have any questions, please feel free to ask them during office hours or contact me at other times via email or via a phone appointment.

Course Calendar – Summer 2018

All activities are due by 11:59 p.m. on the due date listed below*

Week 1: June 11 - 17
Unit 1: User Security Awareness and Fraud

Activity	Due Date
Read *Security Planning: An Applied Approach:* Read Chapters 1-2.	
Watch the Security Awareness Commentary and complete the Self-Checks	
Complete the Security Awareness quiz	
Watch the Introduction to Fraud Commentary and complete Self-Check	
Complete the Fraud quiz	Complete by: **Thursday, June 14**
Participate in the Unit 1 Class Discussion: Applying Security to My Industry	Post initial messages by: **Thursday, June 14** Post responses by: **Sunday, June 17**
Complete Unit 1 Case Study assignment	Post initial messages by: **Thursday, June 14** Submit Group Summary to Dropbox by: **Sunday, June 17**

Week 2: June 18 - 24
Unit 2: Identifying and Controlling Risk

Activity	Due Date
Read Security Planning: An Applied Approach: Read chapter 4 on risk and chapter 14 on HIPAA.	
Watch the Risk Management Commentary and complete the Self-Check	
Read the HIPAA Commentary	
Complete the Risk quiz	Complete by: **Thursday, June 21**
Participate in the Unit 2 Class Discussion: Applying Risk to My Industry	Post initial messages by: **Thursday, June 21** Post responses by: **Sunday, June 24**
Complete the Unit 2 Case Study Assignment	Post initial messages by: **Thursday, June 21** Submit Group Summary to Dropbox by: **Sunday, June 24**

Week 3: June 25 – July 1
Unit 3: Business Continuity

Activity	Due Date
Read Security Planning: An Applied Approach: Read Chapter 5: Addressing Business Impact Analysis and Business Continuity	
Watch the Business Continuity Commentary and Complete the Self-Check	
Complete the Business Continuity quiz	Complete by: **Thursday, June 28**

Complete the Unit 3 Discussion: Applying Business Continuity to My Industry	Post initial messages by: **Thursday, June 28** Post responses by: **Sunday, July 1**
Complete the Unit 3 Case Study Assignment	Post initial messages by: **Thursday, June 28** Submit Group Summary to Dropbox by: **Sunday, July 1**

Week 4: July 2 - 8
Unit 4: Information Security

Activity	Due Date
Read Security Planning: An Applied Approach: Chapter 7: Designing Information Security	
Watch the Information Security Commentary and Complete the Self-Check	
Complete the Info Security quiz	Complete by: **Thursday, July 5**
Complete the Unit 4 Discussion: Controlling Data Access	Post initial messages by: **Thursday, July 5** Post responses by: **Sunday, July 8**
Complete the Unit 4 Case Study Assignment	Post initial messages by: **Thursday, July 5** Submit Group Summary to Dropbox by: **Sunday, July 8**

Week 5: July 9 - 15
Unit 5: Network Security

Activity	Due Date
Read Security Planning: An Applied Approach: Chapter 8 Planning for Network Security	
Watch the Network Security Commentary and Complete the Self-Check	
Complete the Network Security quiz	Complete by: **Thursday, July 12**
Complete the Unit 5 Discussion: Applying Network Security to My Industry	Post initial messages by: **Thursday, July 12** Post responses by: **Sunday, July 15**
Complete the Unit 5 Case Study Assignment	Post initial messages by: **Thursday, July 12** Submit Group Summary to Dropbox by: **Sunday, July 15**

Week 6: July 16 - 22
Unit 6: Physical and Personnel Security

Activity	Due Date
Read Security Planning: An Applied Approach: Chapter 9: Designing Physical Security; Chapter 10: Organizing Personnel Security.	
Watch the Physical Security Commentary and Complete the Self-Check	

Read the Personnel Security Commentary	
Complete the Physical Security quiz	Complete by: **Thursday, July 19**
Complete the Unit 6 Discussion: Developing a Code of Ethics	Post initial messages by: **Thursday, July 19** Post responses by: **Sunday, July 22**
Complete the Unit 6 Case Study Assignment	Post initial messages by: **Thursday, July 19** Submit Group Summary to Dropbox by: **Sunday, July 22**

Week 7: July 23 - 29
Unit 7: Incident Response

Activity	Due Date
Read Security Planning: An Applied Approach: Chapter 11	
Watch the Incident Response and Complete the Self-Check	
Complete the Incident Response quiz	Complete by: **Thursday, July 26**
Complete the Unit 7 Discussion: Applying Incident Response to My Industry	Post initial messages by: **Thursday, July 26** Post responses by: **Sunday, July 29**
Complete the Unit 7 Case Study Assignment	Post initial messages by: **Thursday, July 26** Submit Group Summary to Dropbox by: **Sunday, July 29**