MIS 5206 – Protecting Information Assets - Syllabus

Instructor Information		Greg Senko greg.senko@Temple.edu					
Office Information		Alter Hall 239					
Office Hours		By Appointment (typically before class on Thursday)					
CRN	24972	**Section**	1	**Location**	Alter 239	**Time**	Tuesday 5:30 – 8:00

Course Objectives

In this course you will gain an understanding the importance of and techniques related to managing information assets including logical, physical, and environmental security along with disaster recovery and business continuity.

The Key subject areas that are covered in the course are:

1. Information Security Risk Identification and Management
2. Security Threats and Mitigation Strategies

The first half of the course, leading up to the mid-term exam, will focus on Information Security Risk Identification and Management. The second half of the class will cover the details of security threats and the mitigation strategies that are used to mange risk.

Grading

Item	Percent of Total Points
Participation	20%
Case Analysis Reports	30%
Mid-Term Exam	25%
Final Exam	25%
Total	**100%**

Participation

Much of your learning will occur as you prepare for and participate in discussions about the course material. The assignments, cases, and readings have has been carefully chosen to bring the real world into class discussion while also illustrating fundamental concepts.

To encourage participation, 20% of the course grade is earned by preparing before class and discussing the topics between and in class. Evaluation is based on you consistently demonstrating your engagement with the material. Assessment is based on what you contribute, not simply what you know.

1) ***Preparation before class*** – To facilitate active participation in the class I request that you do the following before noon on the day of the class:

   Briefly address and summarize:

   a. One key point you took from each assigned reading. (One or two sentences per reading)
   b. One question that you would ask your fellow classmates that facilitates discussion.

   I will also require that you identify, and are prepared to discuss, an article about a current event in the Information Security arena each week. Each student is

expected to contribute a link to an article to the online class discussion each week. An ideal article would be tied thematically to the topic of the week. However, any article you find interesting and would like to share is welcome. The deadline for posting is noon on the day of class.

2) **Participation during class** – We will typically start each session with "opening" questions about the assigned readings and case study. I may ask for volunteers, or I may call on you. Students called on to answer should be able to summarize the key issues, opportunities, and challenges in the case study. All students should be prepared to answer these questions.

   Another important aspect of in-class participation is completion of in-class assignments and contribution to any break out activities.

3) **Participation between classes** – To facilitate ongoing learning of the course material, we will also discuss course material on the class blog in between class. You will post case study analyses to the course website. Reading and commenting on these analyses will further the quality of our in-class discussions.

The criteria for participation includes attendance, punctuality, level of preparation, professionalism, answering questions, discussing readings, discussing case studies, contributing to group activities, and contributing to a positive learning environment. Recognizing that students sometimes have unavoidable conflicts, the baseline for expected participation is assessed on one less week than the number of assigned weekly write-ups.

Case Study Analyses

You will officially prepare two case studies that I assign you during the semester. For each case study I will provide several discussion questions. Pick one question and respond to it in depth. Your analysis should not exceed one single-spaced page using 11 point Times New Roman font with one-inch margins. Do not prepare a separate cover page, instead put your name, the class section number (MIS5206.001), and the case name in the top-left corner of the header.

To submit your case study analysis, you must post it on the class blog no later than **Monday at 8:00 AM** of the week it is due. Please copy your analysis in clear text onto the blog.

Late submissions for this deadline will result in no credit earned for this assignment.

There is no one particular style for a good case study analysis. But, there are some common elements to excellent submissions (additional, grade-specific criteria are provided at the end of this syllabus):

- The opening of the analysis makes it immediately clear which case study and what question is being addressed.

- You have cited specific details regarding key facts and issues of the case. Instead of general observations about information technology or organizations that apply to any

problem, draw details from the case study itself. Analyses, observations, and suggestions should be tied directly to those key facts and issues. You can also draw on the other readings in the course to inform and support your arguments.

- After analyzing the details of the case study, discuss how its specific issues have broader application. In other words, use your analysis to provide some advice to managerial decision-makers that can be applied to other situations beyond this case.

- Provide a balanced perspective. For example, when making a recommendation explain the pros and cons, providing both the rationale (the why) as well as its feasibility (the how). Well-considered recommendations include discussion of potential issues with your solution and conditions that should be in place for your recommendation to be successful.

Exams

We will have a mid-term exam that covers the Information Security Risk Management materials that we will address in the first 5 weeks of the semester. It will have both multiple choice and essay components. It represents 25% of your final grade.

Final Exam

The final exam will also both multiple choice and essay components. The exam will be comprehensive. Everything we cover during the semester could appear on the final. The final exam is weighted 25% of your final grade.

Readings	
Text	**Computer and Information Security Handbook, John R. Vacca,** Morgan Kaufmann 2009 (any version will do)
ISACA	**ISACA Risk IT Framework** http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx
	ISACA Assignment 1: "Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans" http://www.isaca.org/Journal/Past-Issues/2002/Volume-1/Pages/Disaster-Recovery-and-Business-Continuity-Planning.aspx
	ISACA Assignment 2: "What Every IT Auditor Should Know About Backup and Recovery" http://www.isaca.org/Journal/Past-Issues/2011/Volume-6/Pages/What-Every-IT-Auditor-Should-Know-About-Backup-and-Recovery.aspx
SANS	**SANS Assignment 1: "**The Importance of Security Awareness" Training **https://www.sans.org/reading_room/whitepapers/awareness/importance-security-awareness-training_33013**
	SANS Assignment 2: "Making Security Awareness Work for You" https://www.sans.org/reading_room/whitepapers/awareness/making-security-awareness-efforts-work_32763
	SANS Assignment 3: "Implementing Robust Physical Security" http://www.sans.org/reading_room/whitepapers/physcial/implementing-robust-physical-security_1447
	SANS Assignment 4: "Assessing Vendor Application Security A Practical Way to Begin" http://www.sans.org/reading_room/whitepapers/application/assessing-vendor-application-security-practical_1370
	SANS Assignment 5: "Application Development Technology and Tools: Vulnerabilities and threat management with secure programming practices, a defense in-depth approach" http://www.sans.org/reading_room/whitepapers/application/application-development-technology-tools-vulnerabilities-threat-management-secure-pro_1283
	SANS Assignment 6: "An Overview of Cryptographic Hash Functions and Their Uses" https://www.sans.org/reading_room/whitepapers/vpns/overview-cryptographic-hash-functions_879
	SANS Assignment 7: "The Risks Involved With Open and Closed Public Key Infrastructure https://www.sans.org/reading_room/whitepapers/vpns/risks-involved-open-closed-public-key-infrastructure_882
ISO	**ISO Assignment: 1** ISO 27001 Data Security Classifications http://www.iso27001security.com/ISO27k_Model_policy_on_information_classification.pdf
HBR	***HBR Assignment 1: "**The Myth of Secure Computing" by Robert D. Austin and Christopher A.R. Darby, HBR OnPoint
Cases	**Case materials will be assigned during the semester**

The SANS (System Administration, Networking, and Security) Institute articles are available from the SANS Reading Room at the following link: http://www.sans.org/reading_room/

*The Harvard Business Review material is licensed and must be acquired by the student.