CNS 440 Security Management **Matt Kestian**

Section 901-910 Spring 2014

Instructor Information:

Instructor:	Matt Kestian
Office:	CDM 230
Office Hours:	Tuesday evening from 5:15 pm – 5:45 pm and 9:00 pm -10:00 pm (If you are not available during this time, please email me to schedule an appointment)
Preferred Email:	mkestian@cdm.depaul.edu

Course Description:

Survey of information security considerations as they apply to information systems analysis, design, and operations. Topics include information security vulnerabilities, threats, and risk management; security policies and standards; security audits; access controls; network perimeter protection, data protection; physical security; risk management, security education training and awareness. Laboratory exercises will be used to illustrate concepts and security tools widely used by professionals.

Course Information:

Days and Time:	Tuesday evening from 5:45 pm – 9:00 pm
Location:	CDM 230
Course Web page:	https://col.cdm.depaul.edu/

Required Textbook:

Fundamentals of Information Systems Security, by Kim and Solomon. DO NOT BUY THIS BOOK. It is available for free on DePaul Libraries, Safari Books Online. The link to the DePaul Libraries site is http://www.library.depaul.edu/Find/resourceList.aspx?s=89 . Click on the link to Safari Books Online and search for Fundamentals of Information Systems Security. You will also need the Virtual Lab Access from the publisher, Jones & Bartlett Learning. I am working with the publisher to get access to the virtual lab environment. There will be a charge to purchase the lab access.

We will be using DePaul's e-library Books 24x7 for resources related to the homework assignments. DePaul students can access Books 24x7 (for free!) using the following link. Use your Campus Connect to login. https://login.ezproxy2.lib.depaul.edu

Course Objectives:

At the end of this class you will be able to understand Information Security:

- Concepts and terminology
- Attack vectors
- Risk Management
- Governance
- Technologies
- Related security concepts (e.g., Physical Security, Legal, Regulatory, etc.)

Course Structure:

Your participation will be crucial to your learning experience. A lot of questions will be asked to you and you are expected to do the same to the instructor and your peers. When confused or frustrated about a topic, use the instructor and your peers as resources. You will be surprised by how much you will learn from your classmates. In addition to the work we will do in class, you are also expected to do work at home or in the lab on your own. Make sure you plan ahead and budget your time accordingly.

VMware:

This course will have hands-on exercises designed to educate students on technology and techniques used in security. In order to facilitate this in a safe environment, you will need to have a computer available with VMware installed. VMware allows you to run virtual computers that have security tools installed. http://en.wikipedia.org/wiki/Virtual_machine

Grading:

Class Participation 10% - You will be assigned in-class activities or mini case studies to help reinforce course concepts and terminology. You will perform these during class and also present on topics to the class. Your participation factors into your overall grade.

Homework 50% - Expect five (5) assignments/projects to be submitted **before class (5:45 p.m. CST) on Wednesdays**. Each assignment will have a point allotment; to get full credit, each assignment must:

1. Be completed in accordance with, and fulfill all the required specifications listed in the assignment.
2. Responses must have substance and be relevant to the question.
3. Use the assignment posted in COL as a template; include your name, insert appropriate screenshots where indicated, and responses under each question.
4. Be submitted through COL before the deadline. I will not accept any assignments via email. It is every student's responsibility to ensure the timely completion of each assignment.

Late assignments will not be accepted. NO EXCEPTIONS since we will be reviewing the assignment at the start of each class.

Final Group Project 40% - Students will form teams and conduct advanced research of information security technologies then write a procedure on how to test the technology. Instructions and more detail will be provided later during the quarter. 'Advanced' means the topic was not covered in class.

Grading Standards:

Letter Grade	Minimum % of Total Points	Letter Grade	Minimum % of Total Points
A	92.00	C+	78.00
A-	90.00	C	72.00
B+	88.00	C-	70.00
B	82.00	D+	68.00
B-	80.00	D	60.00
		F	0.00

Incomplete Grade: An incomplete grade is given only for an exceptional reason such as a death in the family, a serious illness, etc. Any such reason must be documented. Any incomplete request must be made at least two weeks before the final, and approved by the Dean of the School of CDM. Any consequences resulting from a poor grade for the course will not be considered as valid reasons for such a request.

Academic Integrity: This course follows the Academic Integrity Policy of DePaul University.

Students with disabilities:
If you need an accommodation owing to a disability, please contact the instructor the first week of class.

Changes to Syllabus: This syllabus is subject to change as necessary during the quarter. If it occurs, it will be thoroughly addressed during class.

CNS 440 Security Management **Matt Kestian**
Section 901-910 Spring 2014

Week by week detailed breakdown (Please read the materials before the class period):

Week 1: Introduction to Information Security Management
Topics include: Course Introduction, Homework Structure, Why security is important, Security Education, Managing Information Security in today's environment.
Lab Setup: Creating your virtual lab environment using VMware

Week 2: Attack Vectors and Threats
Topics include: Who the bad guys are, how they abuse computer systems, and what they are after.

Week 3: Risk Management
Topics include: Learn how to identify risk, document it, and measure it.
Assignment 1: Conduct a risk assessment

Week 4: Operational Security
Topics include: Policy/Standards/Procedures, Access Control (PKI), Cryptography, Security Blueprints, Frameworks, Security Awareness and Training, Incident Response, Business Continuity and Disaster Recovery, Personnel Security, Data Classification and need to know, Penetration Testing, etc.
Assignment 2: Password auditing using John The Ripper (JTR)
Case Study: Stuxnet

Week 5: Technical Controls Part 1 (Host Security)
Topics include: Asset Inventory of Software, Secure Configurations for Information Systems, Malware Defenses, Account Management, Log Monitoring, etc.
Assignment 3: Active Information Gathering using Nmap

Week 6: Technical Controls Part 2 (Network Security)
Topics include: Asset Inventory of Hardware, Wireless, Network Device Configurations, Tiered Networks, Boundary Defenses, Network Protocols, Data Loss Prevention (DLP), etc.
Case Study: Operation Aurora
Assignment 4: Analyzing network traffic using Wireshark

Week 7: Technical Controls Part 3 (Application Security)
Topics include: Vulnerability Assessments, OWASP Top 10, Secure Coding Practices, etc.
Assignment 5: Exploring web application vulnerabilities using DVWA
Final Project Assigned: Advanced research project

Week 8: Physical Security, SCADA, and VOIP Systems
Topics include: Review of various types of physical security controls, how they relate to information security, and other potential devices connected to the network that people do not commonly assess or think of.

Week 9: Legal, Regulatory, and Privacy Considerations
Topics include: This lecture will cover various types of laws that address cyber-security, the regulatory landscape enforcing laws for various industries, Payment Card Industry, and Privacy.

Week 10: Validate and Sustain the Security Program
Topics include: Key take-aways professionals must consider to ensure the security program put in place stays current and matures. Discussion will focus on metrics, reporting, and governance.