DEPAUL | COLLEGE OF COMPUTING AND DIGITAL MEDIA

Course Information

Course ID: CNS440
Name: Information Security Management
Quarter: Fall 2016-2017
Meeting time: Monday 5:45PM - 9:00PM
Location: LEWIS 01217 at Loop Campus

Instructor Information

Instructor: Filipo Sharevski
Office: Loop Campus, CDM 750
Office Hours: http://www.cdm.depaul.edu/about/pages/people/facultyinfo.aspx?fid=1341
Other times by appointment (email/text me with your request)
Office Telephone: Loop - 312-362-1075
Email: fsharevs@cdm.depaul.edu
Mobile: 765-714-9574
Skype : filipotech

Important Dates

September 13, 2016	Last day to add (or swap) classes to AQ2016 schedule
September 20, 2016	Last day to drop classes with no penalty.
September 20, 2016	Last day to select pass/fail option
September 21, 2016	Grades of “W” assigned for classes dropped on or after this day
October 25, 2016	Last day to withdraw from AQ2016 classes
November 16, 2016	End AQ2016 quarter. All assignments due.

Textbook

Fundamentals of Information Systems Security, Second Edition, David Kim and Michael G. Solomon, Jones & Bartlett Learning, ISBN: 978-1-284-03162-1. We will be using the applied labs that are available with the text.

Course Description

Survey of information security management as it applies to information systems analysis, design, and operations. Managing information assets and the security infrastructure. Emphasis on managing security-related risk, as well as the process of developing, implementing, and maintaining organizational policies, standards, procedures, and guidelines. Identifying and evaluating information assets, threats, and vulnerabilities. Quantitative and qualitative risk analysis, risk mitigation, residual risk, and risk treatment as they relate to information security. Topics include information security vulnerabilities, threats, and risk management; security policies and standards; security audits; access controls; network perimeter protection, data protection; physical security; security education training and awareness. Introduction to compliance, as well as the CISSP domains.

Course Objectives

At the conclusion of the course, students will be able to:

- Understand and contextualize the principles of information security – confidentiality, integrity and availability
- Understand, implement and develop cybersecurity protection techniques, information security policies and information security programs
- Understand and implement cybersecurity risk management
- Plan a security awareness, training and education activity
- Think critically about:
    - Role of a cybersecurity expert
    - Broader set of factors affecting the information security management
- Respond in face of new cybersecurity exploits, campaigns, latest trends, and challenges

Agenda

Week	Date	Topic	Assignment	Reading
Week 1	09/12/2016	**Course Overview and Logistics** **Information Security Environment:** Security Basics - Principles, Cybersecurity Predictions for 2016 – midyear review	Homework – Chapters 1 & 2 Review /	Chapters 1 & 2
Week 2	09/19/2016	**Information Security Planning:** Security Basics – Access Control and Cryptography Information Security Planning, *Cyber Insecurity* – the Case of Stuxnet	Homework – Chapters 5 & 9 Lab 1 - Performing Reconnaissance and Probing using Common Tools	Chapters 5 & 9
Week 3	09/26/2016	**Threats and Vulnerabilities**: Threats and Vulnerabilities overview, *Cyber Insecurity* – the Case of Target Breach	Homework – Performing a Threat Assessment Lab 2 - Performing a Vulnerability Assessment	Chapters 3 & 4
Week 4	10/03/2016	**Risk Assessment:** Defining Risk in Information Security, Risk Quantification	Homework – Chapter 8 Lab 3 - Enabling Windows Active Directory and User Access Controls	Chapter 8; NIST SP 800-30
Week 5	10/10/2016	**Risk Assessment:** Enterprise Risk Management; *Cyber Insecurity* – the Case of Ashley Madison Breach and the Security Mirage	Homework – Risk Analysis Lab 4 - Using Group Policy Objects and Microsoft Baseline Security Analyzer for Change Control	Chapters 10 & 11 ISACA caselets

Week 6	10/17/2016	**Security Policies:** Standards, Guidelines and Approaches for Protection of Organizational Assets; Technical Controls; Physical Security	Homework – Security Policy Lab 8- Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities	Chapter 6 & 12
Week 7	10/24/2016	**Security Education, Training and Awareness:** Social Aspects of Information Security; *Cyber Insecurity* – the Case of Glibc	/ Lab 9 - Eliminating Threats with a Layered Security Approach	Chapters 13 & 14
Week 8	10/31/2016	**Security Program Validation / Ethics and Regulation**	/ /	Chapter 7
Week 9	11/07/2016	**Presentations**		
Week 10	11/14/2016	**Presentations**		

Grading

Grading is based on the manner in which you fulfill the objectives of this course. I will grade all your assignments on a percentage basis, which I will then convert to a letter. I will convert percentages to letters based on the following schedule:

Percentage Grade	Letter Grade	Manner of fulfillment
92-100	A	Excellent
90-91	A-	
88-89	B+	
82-87	B	Very Good
80-81	B-	
78-79	C+	
72-77	C	Satisfactory
70-71	C-	
68-69	D+	
62-67	D	Poor
60-61	D-	
0-59	F	

The weights of each assignment for contributing to the final average are as follows:

Assignment	Weight in final grade
Homework	40%
Labs	25%
Discussion	5%
Story Time	10%
Paper	15%
Presentation/Critiques	5%

Assignments Delivery

Homework is due a week after each is assigned at 11:59 PM. I will accept late homework according the following schedule:

$$p = \log_2(2 - \frac{d}{14})$$

where *p* is the percentage applied to the earned grade and *d* is the number of days the homework is submitted late. After 14 days, homework receives no credit.

Laboratory Exercises

We will use the assignments available from the virtual labs environment available with the text book. We will cover them in class the week after they are assigned. As such, I will not accept late labs. These labs are designed for you to work individually, however, I encourage collaboration and working in groups. Your reports stay individual, though, and I expect to recognize clear engagement with the lab contents on your side.

Discussion

Each class, I will present a current issue related to class topics. We will discuss in small groups, then gather to discuss as a full group. Your participation in such discussions will be evaluated accordingly.

[Online Students only] You will observe the discussion and provide input through the appropriate D2L forum.

Story Time

Each student will be responsible for presenting an article (only once during the quarter), chosen by them, to the class. There will be a Doodle pool at the beginning of the class.

[Online Students only] You will deliver your article and presentation for me to present

Final Paper

There will be a final white/research paper due near the end of the course. This will be a paper on a topic of your choosing in the area of cybersecurity. You can provide detail analysis of a cybersecurity problem and available/potential solutions, survey current challenges and issues, or conduct an actual cybersecurity research and report the results. The topic has to be communicated with me no later than the second week of the semester in order to be approved. Working in groups not more than two are paper/project specific and require prior approval from me. To successfully complete this assignment, you will have to read and include content from published papers, books, and validated information sources outside of the reading material available for the course. Use DePaul's University Library as a rich repository for wide range of scientific papers and content available for free to you as students. There is no page/word count limit, however, the paper is expected to commensurate with an academic-level work. For the paper formatting guidelines and reference citation, see the section below.

Final Presentation

All students will create a slide show/web site on your final paper for the entire class. In addition, you will present your site/show sometime during the last week of class and finals week. There will be no final exam. The presentation will be due at the beginning of the last class of the quarter, and will not be accepted late. Online students will need to have access to presentations to complete their final assignment.

[Online Students only] I will post all presentations and you will be responsible for critiquing three of them as part of your presentation grade

Paper Formatting Guidelines

Papers have to be formatted and delivered according to the template under the "Paper Formatting" section in D2L course page. You can chose either IEEE or APA6 citation format. I encourage usage of citation software (Mendeley, Zotero, EndNote…). You can use a word processor of your choice. If you feel that you need help on the citation part, feel free to consult the citation materials provided, the *Publication manual of the American Psychological Association*, any validated source on IEEE or APA6 citation, or contact me.

Attendance

I expect that you will attend every class; it is the single most important action you can take in mastering the course objectives. You are responsible for material covered, assignments delivered or received, and announcements made in class sessions or on the class web site.

Class Cancellation

Unless DePaul University closes because of weather, we will have class.

Incompletes

Students must formally request an incomplete by filling out an Incomplete Grade Request Form.

Academic Integrity

I expect that you have read and understood DePaul's policy on Academic Integrity (http://academicintegrity.depaul.edu/). It is part of this syllabus; follow it.

Changes to Syllabus

This syllabus is subject to change as necessary to better meet the needs of the students. Significant changes are unlikely, and will be thoroughly addressed in class. Minor changes, especially to the weekly agenda, are possible at any time. You will be informed of all such changes.

Tips

1. Writing a scientific paper is a time-consuming and intensive task. Don't procrastinate after we decided on your paper topics and wait until the last week to start searching for material and writing. Feel free to ask for suggestions during your researching and writing process, I am glad to help.

2. Don’t be afraid to approach for help on any issue if you are experiencing any learning difficulties. I don’t want you to gradually fall behind over the semester until things become untenable.

3. Participate actively in discussion sections. Developing critical thinking skills – essential for getting into the cybersecurity mindset – is through interactive learning and class discussions.