DEPAUL | COLLEGE OF COMPUTING AND DIGITAL MEDIA

3/18/18

CNS 440 -Information Security Management

Meeting time: THU 5:45PM-9:00PM **Location:** CDM 224
Type of Instruction: lecture/lecture-discussion/lab

Instructor Information

Instructor: Matt Kestian / mkestian@cdm.depaul.edu / 312-636-5824
Office: Hours: Thu 5:15PM - 5:45PM in office **TBD** and THU 9:00PM – 10:00 PM in CDM 224

Important Dates

April 2	Last day to add (or swap) classes to SQ2018 schedule
April 6	Last day to drop classes with no penalty.
April 7	Grades of "W" assigned for classes dropped on or after this day
May 11	Last day to withdraw from SQ2018 classes
June 1	End SQ 2018 Day & Evening Classes. All assignments due.
June 15	GRADES DUE: SPRING 2018

Textbook

No text book is required. All the readings and papers are posted in D2L for each week.

Laboratory Exercises

We will use a virtual labs environment (see the introductory slides on how to access the 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.

Course Description

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 cybersecurity risk analysis, risk mitigation, residual risk, and risk treatment.

Agenda

Wk	Topic	Assignment	Reading
1	**Course Overview and Logistics** **Information Security Environment:** Security Basics - Principles, Cybersecurity Predictions for 2018	**Homework** – "Information security is information risk management"- critical review /	B. Blakely, E. McDermott, and D. Geer: "Information security is information risk management"
2	**Information Security Planning:** Security Basics – System Security, Security Program Design, Stuxnet	**Homework** – "Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits" - critical review **Lab 1** - Performing Reconnaissance and Probing using Common Tools	F. Greitzer, J Strozer, S. Cohen et al. "Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits"
3	**Threats and Vulnerabilities:** Threats and Vulnerabilities, Verizon Data Breach Report for 2017	**Homework** – Performing a Threat Assessment **Lab 2** - Performing a Vulnerability Assessment	Cybersecurity news
4	**Risk Assessment I**: Mechanics of cybersecurity risk assessment; DDoS risk assessment	**Homework** – "Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale" – critical review **Lab 3** - Enabling Windows Active Directory and User Access Controls	R. Opplinger, "Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale"
5	**Risk Assessment II:** Enterprise Risk Management – Cybersecurity Framework; Security Fatigue	**Homework** – "Identifying How Firms Manage Cybersecurity Investment" – critical review **Lab 4** - Using Group Policy Objects and MBSA for Change Control	T. Moore, S. Dynes, F. Chung "Identifying How Firms Manage Cybersecurity Investment"
	Cybersecurity Risk Assessment		

6	**Security Policies:** Standards, Guidelines and Approaches for Protection of Organizational Assets; Technical Controls;	**Homework** – "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security" critical review **Lab 10** - Implementing an Information Systems Security Policy	S. Boss, L. Kirsch, et al. "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security"
7	**Security Education, Training and Awareness:** Social Aspects of Information Security; People vs. Cybersecurity	**Homework** – Reliable Behavioral Factors in the Information Security Context critical review **Lab 8** - Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities	P Mayer, A. Kunz, M. Volkamer "Reliable Behavioral Factors in the Information Security Context"
8	**Economics of Cybersecurity**: Economic Aspects of Information Security;	**Homework** - Final Paper – Draft Outline **Lab 6** - Implementing a Business Continuity Plan	Writing for College: What is an Academic Paper?
9	**Security Program Validation / Ethics and Regulation**	Prepare your Final Presentation Prepare your Draft Paper	/
10	**Final Papers/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 as:

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	30%
Labs	20%
Cybersecurity Risk Assessment	20%
Paper	25%
Presentation	5%

Assignments Delivery

Homework and Labs are due a week after each is assigned at 11:59 PM. I will accept late homework/labs according the following formula:

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

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/labs receive no credit. No late presentation and paper will be accepted.

Cybersecurity Risk Assessment

As a mid-term assignment, you have to perform an individual cybersecurity risk assessment for a hypothetical company using the NIST Cybersecurity Framework and the NIST Guidelines for Conducting Risk Assessment. I will post the details of the company and you will have to use the tools covered in class to turn a cybersecurity risk assessment worksheet with the risks identified and proposed controls. Be exact in your recommendations. What's a not exact? Recommendations like "Use firewall; do phishing training; use 2-factor authentication". Sure, we know we must use firewall. Configuration? Maintenance? Vendor? This is where you must be exact, and it requires

Final Paper

There will be a final 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. Please read the "Final Paper Minimum Requirements" document in *Course Logistics* module in D2L for the minimum requirements. For the paper formatting guidelines and reference citation, see the section below.

Final Presentation

All students will create a presentation on your final paper for the entire class. In addition, you will present your site/show sometime during the last week of class and/or 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.

Paper Formatting Guidelines

Papers must be formatted and delivered according to the template under the "Paper Formatting" section in D2L course page. You can choose either IEEE, APA6, or MLA 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, or any validated source on IEEE, APA6, or MLA citation. I strongly encourage you to pay a visit or schedule an appointment with the University Center for Writing-Based Learning: http://condor.depaul.edu/writing/

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.

Online Course Evaluations

Evaluations are a way for students to provide valuable feedback regarding their instructor and the course. Detailed feedback will enable the instructor to continuously tailor teaching methods and course content to meet the learning goals of the course and the academic needs of the students. They are a requirement of the course and are key to continue to

provide you with the highest quality of teaching. The evaluations are anonymous; the instructor and administration do not track who entered what responses. A program is used to check if the student completed the evaluations, but the evaluation is completely separate from the student's identity. Since 100% participation is our goal, students are sent periodic reminders over three weeks. Students do not receive reminders once they complete the evaluation. Students complete the evaluation online in CampusConnect.

Academic Policies

All students are required to manage their class schedules each term in accordance with the deadlines for enrolling and withdrawing as indicated in the University Academic Calendar. Information on enrollment, withdrawal, grading and incompletes can be found at: http://www.cdm.depaul.edu/Current%20Students/Pages/PoliciesandProcedures.aspx

Students with Disabilities

Students who feel they may need an accommodation based on the impact of a disability should contact the instructor privately to discuss their specific needs. All discussions will remain confidential. To ensure that you receive the most appropriate accommodation based on your needs, contact the instructor as early as possible in the quarter (preferably within the first week of class), and make sure that you have contacted the Center for Students with Disabilities (CSD) at: csd@depaul.edu. Lewis Center 1420, 25 East Jackson Blvd. Phone number: (312)362-8002

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.

Course Objectives

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

- Understand and contextualize the principles of information security in complex systems and organizations
- Understand, implement and develop cybersecurity controls, security policies, procedures, and programs
- Perform threat, vulnerability and risk assessments
- 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, and latest challenges