CNS 440 - Information Security Management

Meeting time and location: see myCDM
Instructor: Filipo Sharevski / fsharevs@cdm.depaul.edu
Office Hours: Tuesday 1:45 – 4:45. Email me or join the discord server: https://discord.gg/V6QAjP
Type of Instruction: lecture / lecture-discussion / lab

Course Description: Survey of information security management as it applies to information systems analysis, design, and operations: https://www.cdm.depaul.edu/academics/pages/courseinfo.aspx?CrseId=012735

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

- Develop and implement cybersecurity risk management strategies
- Apply the NIST Cybersecurity Framework and the NIST 800-30 Guide for Conducting Risk Assessments to real-world scenarios

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

Homeworks: You need to write a critical review of each assigned paper. There is no minimum or maximum page limit. The grading is based on the substance of your arguments in the review, rather than a simple summary of the article and word/page count. For the last homework you need to write an outline of your paper.

Laboratory Exercises: We will use a virtual labs environment (see the introductory slides on how to access the labs). The labs are designed for you to work individually.

Final Paper: There will be a **final research paper** as your **term assignment**. This will be a paper on a topic of your choosing in the area of cybersecurity. Please read the "Final Paper Minimum Requirements" document in the *Course Logistics* module in D2L for deliverables and formatting. To produce an academic-level research paper, I strongly encourage you to schedule an appointment with the University Center for Writing-Based Learning: http://condor.depaul.edu/writing/

Final Presentation You have to create a presentation on your final paper for the entire class. It has to be no more than 5-6 slides, containing only the contribution of your work.

Assignments Delivery: Assignments are due one week after each is assigned at 11:59 PM. No late submission will be accepted. Absolutely no grade bargaining will be allowed.

Grading: Grading is based on a percentage basis, which convert to a letter as:

Percentage	Grade	Percentage	Grade	Percentage	Grade
		100-92	A	91-90	A-
89-98	B+	87-82	B	81-80	B-
79-78	C+	77-72	C	71-70	C-
69-68	D+	67-62	D	61-60	D-
59-0	F				

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

Assignment	Weight in final grade
Homework	20%
Labs	20%
Final Paper	50%
Presentation	10%

Attendance: I expect that you will attend every class; You are responsible for material covered, assignments delivered/received, and announcements made in class/ on D2L.

Class Cancellation: Unless DePaul University officially closes, we will have class.

Incompletes: Must formally be requested using the Incomplete Grade Request Form.

Academic Integrity: You must read, understand, and comply with the DePaul's policy on academic integrity: http://academicintegrity.depaul.edu/ . It is part of this syllabus.

Changes to Syllabus: I reserve the right to make changes to the syllabus.

Academic Policies: All students are required to manage their class schedules each term in accordance with the deadlines indicated in the University Academic Calendar: 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 Center for Students with Disabilities (CSD) at: csd@depaul.edu.

Preferred Name & Gender Pronouns: I will gladly honor your request to address you by an alternate name or gender pronoun: http://policies.depaul.edu/policy/policy.aspx?pid=332

Agenda:

Wk	Topic	Assignment
1	**Course Overview and Logistics Cybersecurity Fundamentals**	**Homework 1** – "So long, and no thanks for the externalities: the rational rejection of security advice by users"
2	**Information Security Management Fundamentals**	**Lab 1** - Performing Reconnaissance and Probing using Common Tools
3	**Threats and Vulnerabilities**	**Lab 2** - Performing a Vulnerability Assessment
4	**Risk Assessment I**	**Homework 2** – "Risk Homeostasis in Information Security: Challenges in Confirming Existence and Verifying Impact"
5	**Risk Assessment II**	**Lab 3** - Enabling Windows Active Directory and User Access Controls
6	**Security Policies and Decision Making**	**Lab 6** - Implementing a Business Continuity Plan
7	**Security Education, Training and Awareness**	**Homework** 3 – "Against Mindset"
8	**Economics of Cybersecurity**	**Lab 10** - Implementing an Information Systems Security Policy
9	**Ethics and Regulation**	**Homework** 4 – Paper Outline and References
10	**Final Presentations**	Present your work