Introduction to Information Security Management
MISM Course S22-95752Z
Spring 2022

Carnegie Mellon University

Instructor: Randy Trzeciak
Office: Hamburg Hall 1104C
Office hours: By Appointment
Phone: 412-268-7040
E-mail: randallt@andrew.cmu.edu

TA: TBD
Office hours: Refer to Course Site
E-mail: TBD

Web site: ***http://www.cmu.edu/canvas/***

Course Management

All course materials will be managed through Canvas. Canvas will be used to post announcements of assignment and other information. Please be sure to check these announcements frequently to ensure you have the latest information about the course.

Textbooks

- Pfleeger, Charles P., Pfleeger, Shari L., and Margulies, Jonathan. *Security in Computing 5th Edition*. Upper Saddle River, NJ: Prentice Hall, 2015. Print *ISBN:978-0-13-408504-3 (SC) (REQUIRED)*

https://www.oreilly.com/library/view/security-in-computing/9780134085074/?ar

When prompted to "Select your institution", select "Not Listed? Click here.". Enter your CMU Andrew email address and password, when prompted for your "Academic email".

- Rice, David. *Geekonomics: The Real Cost of Insecure Software*. Upper Saddle River, NJ: Pearson Education, 2008. Print *ISBN: 978-0-32-21735973 (GS) (OPTIONAL)*

https://www.oreilly.com/library/view/geekonomics-the-real/9780321477897/?ar

When prompted to "Select your institution", select "Not Listed? Click here.". Enter your CMU Andrew email address and password, when prompted for your "Academic email".

Prerequisite and Requirements:

None

Course Description

This course is intended to give students an introduction to a variety of information and cyber security topics. As an introductory course, it will cover foundational technical concepts as well as managerial and policy topics. The purpose of the course lectures, assignments, reading, in-class presentations, and examinations are to ensure students have sufficient technical awareness and managerial competence that will enable them to pursue advanced study in information security policy and management as they progress through their program. There is no prerequisite for this course, however successful students will have fundamental knowledge of information and computer systems, and a general awareness of security issues in these systems.

Learning Objectives

Upon completion of this course, the student will obtain an understanding and will apply key concepts, including:

Learning Objective(s)
Foundational concepts of cyber and information security and the key practices and processes for managing security effectively.
Basic network fundamentals – including (but not limited to) topologies, protocols, address conservation, and services, and the security issues that affect networks.
Basic cryptology and why it is fundamental to computer and information security.
Software program deficiencies and the vulnerabilities associated with them.
Access controls and authentication as they are used to secure systems and how they can be mitigated.
Security vulnerabilities that affect operating systems and how they can be mitigated.
The use of risk management to plan, implement, and administer security programs and processes.
The key elements of incident management; detection, remediation, and recovery.
How to translate security into a business driver that is critical to meeting the organization’s mission.
Legal, ethical, and regulatory issues that shape policy development and the ways in which organizations implement and administer security.
The organizational and societal costs of insecurity software.

Each learning objective will be assessed via the following mechanisms: Feedback during lectures; assignments; discussion of reading assignments; reports; presentations; and examinations.

Schedule *(tentative…subject to change during semester)*

Course Week	Lecture Topic	Readings/References
January 17	*Course Administration* *Introduction*	SC: Forward SC: Chapter 1
January 24	*Introduction (cont.)* *Vulnerability Management*	SC: Forward SC: Chapter 1 GC: Chapter 1 & 2
January 31	*Program Security, Part 1*	SC: Chapter 3
February 7	*Program Security, Part 2*	SC: Chapter 3 GC: Chapter 3
February 14	*Operating System Security*	SC: Chapter 5
February 21	*Web Security, Part 1* *Web Security, Part 2*	SC: Chapter 4 GC: Chapter 4
February 28	***Mid Term Exam – Date TBD***	
March 7	*Database Security*	SC: Chapter 7 GC: Chapter 5
March 14	*Network Security, Part 1*	SC: Chapter 6
March 21	*Network Security, Part 2*	SC: Chapter 6
March 28	*Elementary Cryptology*	SC: Chapter 2 SC: Chapter 12
April 4	*Cloud Computing*	SC: Chapter 8 GC: Chapter 6
April 11	*Incident Management* *Risk Management*	SC: Chapter 10 GC: Chapter 7
April 18	*Privacy* *Legal Issues and Ethics*	SC: Chapter 9 SC: Chapter 11
April 25	*Privacy* *Legal Issues and Ethics*	SC: Chapter 9 SC: Chapter 11
May 2	***Final Exam – Date TBD***	

Assignments

There will be **three** homework assignments and each will be focused on analysis of topics relevant to the course lectures and current events in cyber and information security. Each assignment will be announced on Canvas with requirements for submission.

Students will only have 2 weeks after an assignment or exam is returned to question or challenge a grade. After the two week challenge period, the grade will not be changed. Please contact the instructor if you wish to question a grade.

Mid Term Exam

The midterm exam will cover material from the first half of course. The exam will be scheduled during week 7 (February 28) (approximately), with an exact date to be determined during week 3. The exam will be delivered via Canvas and you will have 48 hour period during the mid-term examination week to take the 1 hour (approximate, to be determined) exam.

Final Exam

The final exam will cover material primarily from the second half of the course. The exam will be scheduled during week 15 (May 2), with an exact date to be determined during week 9. The exam will be delivered via Canvas and you will have 48 period during the mid-term examination week to take the 1 hour (approximate, to be determined) exam.

Research Report

Students of management and policy must gain skills and confidence in expressing difficult technical and managerial concepts to decision and policy makers, particularly those who provide funding for key organizational initiatives. For this reason, students in this course will develop a paper based upon readings from publically available sources that will demonstrate his/her ability to communicate technical constructs/challenges/issues clearly and effectively.

Literature Review: Information Security Incident Analysis, Summarization, Presentation

Students of management and policy must gain skills and confidence in expressing difficult technical and managerial concepts to decision and policy makers, particularly those who provide funding for key organizational initiatives. For this reason, students in this course will develop an executive report AND briefing (presentation file), to be recorded (uploaded into canvas) and viewed by instructor, on a security incident described in publically available information.

Extra Credit (*OPTIONAL*)

Student will have two opportunities to obtain additional points, to be added to your mid-term exam and final exam by writing a 1-page executive summary on a cybersecurity current event/issue/topic. Students must submit extra credit submission one no later than TBD and submission two no later than TBD. Additional guidance will be provided.

Evaluation Method

Assignments	15%
Incident Analysis	15%
Mid-Term Exam	25%
Final Exam	25%
Semester Paper	20%
Total	100%

Grading Scale

100 – 98	A+	81 – 80	B-
97 – 92	A	79 – 78	C+
91 – 90	A-	77 – 72	C
89 – 88	B+	71 – 70	C-
87 – 82	B		

Grade Distribution

I plan on using the Heinz School guidelines in deciding on the overall grade distribution. Accordingly, the average grade will be an A-. However, I grade on an absolute scale. If every student does well in the class, each will get an A+ regardless of the recommended grading scale. The same holds true on the other end of the scale.

Late assignment policy

I WILL NOT accept late homework unless the student has made arrangements with me prior to the assignment's due date. *PRIOR ARRANGEMENTS MUST BE MADE NO LATER THAN 12 PM ON THE DUE DATE.*

Policy on cheating and plagiarism

For all submissions for a grade, each student is responsible for handing in his/her own work. For any assignment found to be the partial or complete result of cheating or plagiarism, your grade for that assignment will be zero. Cheating is defined as inappropriate collaboration among students on an assignment or exam or failure to cite others work used in the semester paper or literature review. This can include copying someone else's work with or without alteration. When students are found to be collaborating in this way, *BOTH* will pay the penalty regardless of who originated the work. Please refer to the university's policies: http://www.cmu.edu/policies/StudentPolicy.html

Take Care of Yourself

Do your best to maintain a healthy lifestyle this semester by eating well, exercising, avoiding drugs and alcohol, getting enough sleep and taking some time to relax. This will help you achieve your goals and cope with stress.

All of us benefit from support during times of struggle. You are not alone. There are many helpful resources available on campus and an important part of the college experience is learning how to ask for help. Asking for support sooner than later is often helpful.

If you or anyone you know experience any academic stress, difficult life events, or feel anxiety or depression, we strongly encourage you to seek support. Counseling and Psychological Services (CaPS) is available to help: call 412.268.2922 and visit the website: http://www.cmu.edu/counseling/ . Consider reaching out to a friend, faculty or family member you trust for help getting connected to the support that can help.