MIS 534: Information Security Management

Course Information	**Instructor**: Dr. Jeff Cummings **Office:** CI 2051 **Office Hours:** Tues. and Weds, 9-12 & 2-4 By Appointment **Phone:** 962-3032 (office) **Email:** cummingsj@uncw.edu **Time:** Wednesday 5:30PM - 8:00PM (CI 1013)

Course Overview

Examination of current standards and best business practices in Information Security Management, including planning for security/contingencies, developing a security policy / program, security management, risk management, and protection mechanisms. Topics include evaluation of security models, risk assessment, threat analysis, organizational technology evaluation, security implementation, disaster recovery planning and security policy formulation and implementation.

Textbook and Materials

The field of Information Assurance and Security is constantly changing and evolving. There are standards and guidelines available but brining in recent articles and events is often more beneficial. **We will not have a required textbook** but will instead work from a number of books and sources. All materials you are expected to know will be covered during course lectures and in-class activities. Below is a list of books and resources which will be utilized during the course.

Books and Resources:

Management of Information Security, 5th Edition, Whitman and Mattord, ISBN-10: 1337685690
Fundamentals of Information Systems Security, 2nd Edition, Kim & Solomon (Available on SkillPort)
Information Security: A Practical Guide, Mooney (2015) (Available on SkillPort)
An Introduction to Information Security - NIST Special Pub 800-12

Overall Course Objectives

Upon completion of this course, you will be able to:

1. Define key terms and concepts of information assurance
2. Identify various threats, attacks and vulnerabilities
3. Describe information security legal and ethical issues
4. Conduct risk assessment to identify, analyze and manage risk
5. Develop contingency plans including business continuity, incident response and disaster recovery
6. Identify approaches to access controls, intrusion detection and incident response
7. Identify basic security policies and technologies needed to ensure information security

Note: Emails sent before 5 pm (Monday through Friday) will usually be answered by the end of the same day. E-mails sent after 5 pm (Monday through Friday) or on the weekend will not necessarily be answered the same day.

Evaluation

Exams

There will be two exams over the material covered in the class. The exam will include the lecture material, student presentations, reading assignments/discussion topics and guest speakers when applicable.
No make-up exams will be offered except on medical grounds.

Threat Presentation

The information security landscape continues to change quickly and dramatically. To stay up-to-date on current information security approaches, each student will present a current threat facing organization in the upcoming year. These presentation will be scheduled throughout the semester. More information will be provided in class concerning this assignment.

Class Participation

To truly understand the course material, case studies are provided that address the topic being discussed in class. I will be posting material through Canvas that will help with the discussion during class and students are expected to have read and actively participate during class sessions. Additionally, there will be in-class exercises that you will be completing which will require you to apply some of the material discussed.

Discussion Topics

Every week, there will be discussion topics posted through Canvas. These will typically be current events or areas we may not have time to cover in class. Students are expected to provide an answer to the discussion questions for the module with the expected answer to be 2 to 3 sentences depending upon the question posed. Answers will be graded based on quality and relevance to the topic being discussed.

Term Paper/Project

The primary purpose of this assignment is to provide you an opportunity to further develop practical research skills by investigating an information assurance (IA) related topic (hopefully of personal interest). The only apparent constant in the field of information technology and information assurance is change. Business executives are almost constantly barraged with new technical threats and new technical opportunities. Both line managers and IT managers require an ability to filter this information and attempt to discern threats and opportunities that are truly germane to the interests (strategic or otherwise) of the organization. To do this, managers need not only an in-depth understanding of their organization's current and proposed operations and strategies, but an ability to recognize and evaluate the potential threats and opportunities arising from changes in the environment. Quite frankly, I don't think anyone knows exactly how to educate an individual to recognize such opportunities. However, I am reasonably certain that having the ability to conduct a reasonable business-type analysis of new capabilities should be helpful.

Accordingly, you are to:

1. select a topic from the following list;
2. write a ~3,000 – 4,500 paper regarding the topic
3. include an annotated bibliography (with at least 12 references)
4. give a 15-20 minutes presentation of your executive summary to class.

Presentations will be given during the final exam time. Projects will be assigned on first-come first-served basis. You are encouraged to start early on the project and touch base with the instructor to ensure you are achieving an appropriate level of detail.

Approved Topics include (if you would like to select an alternative topic please check with me first):

- General Data Protection Regulation (GDPR)
- New Trends in Cybersecurity (e.g., Blockchain)
- Control Objectives for Info. and related Technology (COBIT) auditing standards
- Sarbanes-Oxley Act of 2002 (SOX) implications for IT/IA management
- Health Insurance Portability and Accountability Act (HIPAA) implications for IT/IA management
- Cybersecuirty Act of 2015
- Successful approaches to Security, Education, Training and Awareness programs
- Tools
- Identity management
- IA investment analysis
- IA threat analysis
- IA security code checkers
- Secure software development tools
- Trusted computing certification
- Serious Games in Security Education
- Information Technology Infrastructure Library (ITIL) and Security Management
- Recent Attacks (must be approved by instructor first)
- Cryptography

A potential alternative to the term paper will be discussed in class which involves a security analysis of a local business

Miscellaneous

Disabilities

If you have a disability and need reasonable accommodation in this course, you should inform me of this fact in writing within the first week of class or as soon as possible.

If you have not already done so, you must register with the Office of Disability Services in De Paolo Hall (http://www.uncw.edu/disability/students/interested.html) and obtain an Accommodation Letter. You should then meet with me to make mutually agreeable arrangements based on the recommendations of the Accommodation Letter.

Academic Dishonesty Offenses

In this course, we will follow the guidelines of the Academic Honor Code found in Section V of the Student Handbook

Cheating of any kind shall result in a grade of zero (0) on the test, assignment or project in question with a minimum deduction of ONE LETTER GRADE for the class, and a note to the Office of the Dean of Students. The second instance of cheating will result in the grade of an F for the class.

Grading and Grading Policy

The distribution of the grades will be as follows.

Assessments	30%
Threat Topic	10%
Term paper	20%
Discussion Forum	30%
Class Participation	10%

The grading will be based on the following grading scheme (note +'s and -'s are NOT given in this course).

Range	*Grade*
90 – 100	A
80 – 89	B
70 – 79	C
60 – 69	D
< 60	F

The instructor retains the right to subjectively adjust an individual student's grade in appropriate cases, based upon observed performance.

All turned-in assignments will be neatly typed (word-processed) and submitted via Entropy. Specific examples will be provided in class. Students failing to present the information completely, neatly and in the prescribed format will receive minimal credit for their work. Students should double check for spelling and grammar before submitting assignments.

Grades can be viewed using Entropy (***http://csbapp.csb.uncw.edu/entropy/***). Please refer to "Registering Entropy" hand-out to create an account.