Syllabus

Course Title: Cyber Security Principles

Program(s): School of Business

Course #: MIS 645

Catalog Description:

Cyber security is a complex, sophisticated, and growing challenge. This course explores cyber security topics from a business context in alignment with prevailing standards and guidance. The major domains of security are explored from organizational management, risk, and technical perspectives. Critical security goals of Confidentiality, Integrity, and Availability are discussed. The emerging threat landscape is examined, including attacker motives and tactics. The concept of system vulnerabilities is explained along with a review of enterprise techniques for vulnerability management. The security challenge is presented from the enterprise perspective, with attention to the intersection of individual, organizational, and technical cyber security concerns.

Course Objectives:

1. To introduce the fundamental concepts of information and cyber security in the business enterprise.
2. To explore the threats and vulnerabilities associated with business systems.
3. To understand the core domains of security as presented in widely accepted cyber security frameworks.
4. To explain critical cyber security technical components as related to the respective security domains.
5. To introduce cyber risk management concepts.
6. To explore the challenges of communicating cyber security concepts to business executives.
List of Course Outcomes:

1. Students will be able to communicate concepts of cyber security and technical risks to management, executives, and other non-technical audiences.

2. Students will recognize common security goals in information systems.

3. Students will explain characteristics of information or cyber risk in a systems environment.

4. Students will understand prevailing information and cyber security threats.

5. Students will be able to apply common security frameworks to treat cyber risks.

Prerequisites: Having taken an undergraduate course in business information systems or by permission of the instructor.

Cross-listing: NONE

Grading Percentages: Weekly Assignments (10%) ✗  Mid-term (20%) ✗  Final (20%) ✗  Presentation of Final Paper (10%) ✗  Team Project (20%) ✗  Participation (20%) ✗

Final grades will be calculated as follows:

<table>
<thead>
<tr>
<th>Points</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>93 – 100</td>
<td>A</td>
</tr>
<tr>
<td>90 – 92</td>
<td>A-</td>
</tr>
<tr>
<td>87 – 89</td>
<td>B+</td>
</tr>
<tr>
<td>84 – 86</td>
<td>B</td>
</tr>
<tr>
<td>80 – 83</td>
<td>B-</td>
</tr>
<tr>
<td>77 – 79</td>
<td>C+</td>
</tr>
<tr>
<td>74 – 76</td>
<td>C</td>
</tr>
<tr>
<td>70 – 73</td>
<td>C-</td>
</tr>
</tbody>
</table>

Credits: 3 credits  Other
For Graduate Credit toward Degree or Certificate

☒ Yes  ☐ No  ☐ Not for Dept. Majors  ☐ Other

Textbook:


Mode of Delivery  ☒ Class  ☐ Other

Program/Department Ownership:  School of Business

Department Point of Contact:  Paul Rohmeyer, Ph.D.
Babbio Center 414
908-531-2551
prohmeye@stevens.edu

Session Outline:

<table>
<thead>
<tr>
<th>Week</th>
<th>Subject</th>
<th>Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introductions, Foundational Concepts of Cybersecurity in Organizations</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Security Governance, Principles, and Policies</td>
<td>Read Ch. 1-2</td>
</tr>
<tr>
<td>3</td>
<td>Enterprise Resiliency and Business Continuity</td>
<td>Read Ch. 3</td>
</tr>
<tr>
<td>4</td>
<td>Laws, Regulation, and Compliance</td>
<td>Read Ch. 4</td>
</tr>
<tr>
<td>5</td>
<td>Enterprise Information and System Assets</td>
<td>Read Ch. 5</td>
</tr>
<tr>
<td>6</td>
<td>Principles of Cryptography</td>
<td>Read Ch. 6-7</td>
</tr>
</tbody>
</table>
I. PEDAGOGICAL OVERVIEW

A. Method of Teaching

Concepts and theories of security challenges in communications networks and the management of these networks will be taught using a combination of traditional texts, journal articles and the professor’s notes.

Students are required to read all the assigned readings/cases and answer specific assigned questions. The quality and insight of each students comments and the level of engagement in the class discussion are important components of the final grade.
II. ASSIGNMENTS

The following is an overview of your assignments for this class. Assignment details will be provided in Canvas throughout the semester.

20% Weekly Assignments. Assignment details will be posted in Canvas throughout the semester. These are relatively short assignments that are based on class discussion and current events. Feedback will be provided on submissions marked “Incomplete”. Submission is a DOC or PDF document.

20% Midterm: Individual Exam. The Midterm will consist of a series of questions on topics that have been reviewed in class. Submission is a DOC or PDF document.

30% Final: Individual Paper and Presentation. This is an individual research paper that will require you to conduct research using the Stevens online library, or other online libraries of journals and research papers. Exclusive use of Google/Internet searches will not be sufficient to complete your paper. Submission is a DOC or PDF document. Presentation will require a presentation slide deck (PPT).

20% Team Project. This is a team assignment that will require collaboration with your assigned team throughout the semester and presented in class by all group members. Submission is a presentation slide deck (PPT).

10% Participation. Active participation is required to succeed in this course. Requirements to maximize your participation grade are as follows;

- Attendance alone does not represent class participation! Your presence in class is needed, however it is important you are engaged in class discussion and actively prepare to contribute to the class every session. Prepare by reading the text and monitoring information security news sources.
- Missing more than two (2) class sessions during the semester will result in a loss of participation points. Prior notification to the instructor you will miss class is appreciated, however that does prevent the loss of participation points.
- Refrain from using laptops or smartphones during class unless required to do so for in-class assignments. A photo must be uploaded to your Canvas profile. This is mandatory.
- Refrain from speaking with other students during the lectures, or doing anything that is distracting to other class members.
- Further guidance on participation will be provided during class.
Notes on the Final Paper

The final paper is an individual research assignment on a topic that is covered in the class. Topics need to be selected and submitted for approval by week 4. The deliverable is a formal research paper of no less than 12 pages, double-spaced. Illustrations, figures, and tables DO NOT count towards the page total. All externally sourced material must be appropriately referenced using APA referencing format.

The paper should be in a format suitable for submission to industry conferences. Students are encouraged to seek opportunities to present their papers at industry events. Your selected topic should fall into one of the following categories;

- Risk Assessment
- Optimal investment in information security
- Privacy, confidentiality and anonymity
- Interdependent supply chain security
- Intellectual property protection
- Information access and provisioning
- Enterprise Risk Management
- Security standards and regulation
- Behavioral security and privacy
- Cyberterrorism policy
- Organizational security and metrics
- Psychology of risk and security
- Phishing, spam, and cybercrime
- Vulnerability discovery, disclosure, and remediation

Security News Sources

The following are examples of acceptable sources you should monitor throughout the term;

http://www.scmagazine.com/

http://searchsecurity.techtarget.com/

http://www.csoonline.com/

http://www.infosecurity-magazine.com/
III. Stevens Institute Honor Code

The following statement is printed in the Stevens Graduate Catalog and applies to all students taking Stevens courses, on and off campus.

“Cheating during in-class tests or take-home examinations or homework is, of course, illegal and immoral. A Graduate Academic Evaluation Board exists to investigate academic improprieties, conduct hearings, and determine any necessary actions. The term ‘academic impropriety’ is meant to include, but is not limited to, cheating on homework, during in-class or take home examinations and plagiarism."

Consequences of academic impropriety are severe, ranging from receiving an “F” in a course, to a warning from the Dean of the Graduate School, which becomes a part of the permanent student record, to expulsion.

Reference: The Graduate School Catalog, Stevens Institute of Technology