Syllabus

Course Title: Risk Management for Financial Cybersecurity

Program(s): School of Business

Course #: FIN 545

Catalog Description:

This course examines topics related to efforts to maintain security over financial systems within the organization. Students examine recent financial systems breaches, and consider common threats and vulnerabilities related to financial systems. Several methods of risk assessment are explored, as well as the creation of risk treatment strategies, including the design of internal technical and process controls. Students analyze relevant financial services industry regulation and discuss organizational compliance requirements. Response planning is examined for information and cyber security breaches.

Course Objectives:

1. To introduce the fundamental concepts of information and cyber security in the context of financial systems and markets.

2. To lay the foundation for the study of the unique threats and vulnerabilities associated with financial systems and markets.

3. To introduce approaches used to identify and evaluate technology and process risks in financial systems.

4. To list and explain regulatory guidance related to managing risks in financial systems environments.

5. To provide knowledge of actual information and system breach events that have impacted financial systems.

6. To identify and formulate risk treatment options in response to identified financial systems risks.
List of Course Outcomes:

1. Students will recognize common technology and process risk dimensions in financial systems.
2. Students will explain characteristics of the consequences of an information or cyber risk event in a financial systems environment.
3. Students will be prepared to monitor and analyze emerging information and cyber security threats related to financial systems.
4. Students will be able to create treatment options for identified information and cyber risks in financial systems.
5. Students will be able to execute multiple approaches to assess financial systems risk.
6. Students will explain the value of cybersecurity information sharing within the financial services community.

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

Cross-listing: NONE

Grading Percentages: HW (20%) ☒ Mid-term (20%) ☒ Final (25%) ☒ Team Project (25%) ☒ Participation (10%) ☒

Regular attendance in class, and active participation, is expected. 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

Required Textbook:


Required Articles:


References:

FFIEC Cybersecurity Awareness. [https://www.ffiec.gov/cybersecurity.htm](https://www.ffiec.gov/cybersecurity.htm)


**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

**Course Modules:**

<table>
<thead>
<tr>
<th>Lecture</th>
<th>Topics</th>
<th>Reading</th>
<th>Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introductions, Foundational Concepts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Threats</td>
<td>Ch. 1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Vulnerabilities</td>
<td>Ch. 2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Breach Consequences</td>
<td>Ch. 3</td>
<td>Final Paper Topic Due</td>
</tr>
<tr>
<td>5</td>
<td>Breach Probability</td>
<td>Ch. 4</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Cyber Risk Treatment</td>
<td>Ch. 5</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Midterm Review</td>
<td></td>
<td>Midterm Paper Due</td>
</tr>
<tr>
<td>8</td>
<td>Enterprise Cyber Governance</td>
<td>Ch. 6</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Engaging the Organization</td>
<td>Ch. 7</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Continuous Cyber Improvement</td>
<td>Ch. 8</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Learning from Breach Incidents</td>
<td>Ch. 9</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Looking Ahead</td>
<td>Ch. 10</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Individual Presentations of Final Paper</td>
<td></td>
<td>Final Paper Due</td>
</tr>
<tr>
<td>14</td>
<td>Individual Presentations of Final Paper</td>
<td></td>
<td>Team Project Due</td>
</tr>
</tbody>
</table>
PEDAGOGICAL OVERVIEW

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 student’s comments and the level of engagement in the class discussion are important components of the final grade.

SECURITY NEWS AND OTHER PARTICIPATION

A significant portion of your course grade is derived from your level of participation. This course will be most valuable when there are consistent and valuable contributions to the discussion board and conference calls.

***Please note that your attendance in lecture sessions is expected. Missing any more than two (2) scheduled lectures will result in points deducted from your participation grade. Online sessions will be recorded for playback, however your online participation during lectures is expected.***

Therefore, I expect you will actively participate in online discussions, including the posting every week of a summary of one (1) story from technical or media that is about an Information Security topic. Post the URL of the article and 1-2 sentences of explanation about the story. The following are examples of acceptable sources for your articles;

http://www.scmagazine.com/

http://searchsecurity.techtarget.com/

http://www.csoonline.com/

http://www.infosecurity-magazine.com/

https://threatpost.com/

http://www.darkreading.com/

http://krebsonsecurity.com/
ASSIGNMENTS

Individual Assignments

You will be assigned a variety of articles to review and comment. Specific articles and instructions for each assignment will be posted online.

Mid Term

The Mid-Term paper is an individual assignment and is technology focused. Assignment details will be provided during the class.

References and all sources used (articles, texts, Web sites, etc.) must be provided in standard format.

Team Project

Students are assigned to teams and will analyze a recent financial cybersecurity breach incident. Deliverable is a presentation. Further instructions and detail will be provided during the semester.

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. Illustrations, figures, and tables DO NOT count towards the page total. All externally-sourced material must be appropriately referenced using APA referencing format.
Student papers will be presented in class.

**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*