Carnegie Mellon University
95-764: Special Topics: Information Assurance & Security
Spring Semester 2011; Session A3, 6 units

Instructor: Carol A. Sledge, Ph.D.
Office: SEI 5220
Phone: 412-268-7708
Email: csledge@andrew.cmu.edu

IMPORTANT: be sure to include [95-764] at the start of the Subject line (otherwise it might be considered SPAM)

Office Hours: After class and by appointment

Course Meetings
Mondays, 6:30 p.m. - 9:20 p.m.

Required Text

Course Overview
This course is an overview of increasingly important area of information assurance and security. As more and more functionality and dynamic decision-making are pushed down and out into the organization (power to the edge), assurance and security concerns, with their organizational and human dimensions, impact the fidelity of the data and the very survival of the organization. Class sessions will be centered on case studies and discussion. Topics include overview and definitions, protecting employee data, disaster and contingency planning, compliance with federal
information security requirements, tracking a computer intruder, implementing an information security awareness program. Students will leave the course with an understanding of the various concepts and their impacts on the organization.

Pre-requisites: Graduate standing and at least one programming course.

This class is a combination of lecture, readings (case studies), & in-class discussion/presentation of case studies.

Course Expectations and Course Grades

To complete this course successfully, students will be expected to complete the following activities. Weights indicate the contribution to the final course grade.

- [Best] 4 of 6 Quiz grades 40%
- [Best] 5 of 6 Case Study Question Narrative grades 25%
- [Best] 5 of 6 Case Study Question Presentation grades 25%
- CISO paper 5%
- In-class discussion 5%

See also the “Case Study Requirements” and “CISO Paper” information at the end of this section.

From week 2 through week 7 there will be a timed, in-class quiz (open book, open (hardcopy) notebook, open (hardcopy) notes; closed laptops, closed pdas, closed phones, electronic tablets, etc. – see also lecture one) based on information/reading from prior week/class and reading for the current week/class. You cannot make up any in-
class quiz you miss through absence or lateness (note: two of the quizzes can be dropped/missed – the reason for only using the best 4 of 6 quiz grades). These quizzes will be given promptly at 6:30 p.m. and will be collected promptly at the end of the time period allowed for the quiz. Any evidence of collaboration or copying of material between students during the exam will result in a 0 (zero) grade for that exam for all students involved. There will be no midterm or final exam.

Other factors, such as amount of class participation and punctual, regular attendance may be used, at the instructor's option, to make adjustments to final grades. The instructor will assume that you are well prepared for class each week and will feel free to call upon you.

Case Study Requirements

The week before a particular case study is scheduled for discussion, case study questions (located at the end of the case study) will be assigned to each individual.

For each case study, student(s) are required to
1) Submit written answers to each question assigned to them. The answers are due AT THE START OF CLASS the following week (when the case will be discussed) and must be submitted in hardcopy form (digitally printed, NOT handwritten). [Students should also bring a hardcopy for themselves to reference during the class discussion.]
   a. The first page must include the following:
Grading of the narrative will be based on content, spelling, punctuation, sentence structure, grammar, and adherence to instructions/format. Answers are expected to be in a narrative format, not PowerPoint. Answers received after the start of class (6:30) will receive 0 credit. Any evidence of plagiarism, copying of material from the Internet, or other inclusion of materials WITHOUT proper citation in the case study question homeworks will result in a 0 (zero) grade for that work. **There are no make-ups/extra credit.** Each student’s best 5 of 6 case study narrative answers will be used as part of the computation of the final course grade [worth 25% of final course grade].

Additionally, for each case study question, student(s) are required to
2) Prepare a presentation of their answers, which takes place the following week (when the case will be discussed.)
   a. Presentation should be professional, and the use of visuals, such as PowerPoint, is expected.
   b. The PowerPoint slides should not just be a “cut and pasting” of the narrative answer submitted; it should be able to stand alone – i.e. make sense if one did not have the narrative at hand
   c. Each student must clearly identify themselves at the start of their part of the presentation
   d. One hard copy of the presentation (1-up or 2-up format; NOT 3-up or 6-up format) is due to the instructor at the start of the presentation.
   e. Students are expected to use their laptop computers to do the presentation (i.e. the instructor’s laptop is NOT available for student presentations)

Grading of the presentation will be based on content, the level of professionalism displayed in the presentation and adherence to instructions/format. For example, the presentation should not consist of the student reading from the monitor/screen, or from a piece of paper held in front of the student’s face. Any evidence of plagiarism, copying of material from the Internet, or other inclusion of materials WITHOUT proper citation in the case study question homeworks will result in a 0 (zero) grade for that work. **There are no make-ups/extra credit.** Each student’s best 5 of 6 case study presentations will be used as part of the
computation of the final course grade [worth 25% of final course grade].

CISO Paper

Worth 5% of the final grade.

For the 2nd last class session (February 21, 2011) write a paper which takes the viewpoint of a Chief Information Security Officer (CISO) with respect to the following 5 areas (note, these are areas addressed by the case studies):

- Data privacy (including cross border concerns)
- Physical security (and its tie to cybersecurity)
- Contingency planning
- Risk management/risk assessment/legal issues/governance
- Security awareness, education and training

In your report, for each of the above five areas, what questions would you, as the CISO, ask of or what information would you need from each of the following four senior managers?

- Chief Information Officer
- Chief Operating Officer
- Chief Financial Officer
- Chief Legal Officer

A hard copy of the report is due AT THE START OF CLASS on February 21, 2011 and must be submitted in hardcopy form (digitally printed, NOT handwritten). [Students should also make sure they have a hardcopy for themselves.]
Each page of the report must include the following:

i. Student’s full name
ii. The words “CISO paper”
iii. Page number of the hardcopy report (i.e. page 1, 2, etc.)

Grading of this report will be based on content, spelling, punctuation, sentence structure, grammar, and adherence to instructions/format. The report is expected to be in a narrative format, not PowerPoint. Reports received after the start of class (6:30) will receive 0 credit. Any evidence of plagiarism, copying of material from the Internet, or other inclusion of materials **WITHOUT** proper citation will result in a 0 (zero) grade for that work. **There is no make-up/extra credit.** (See also the initial executive roles articles – both available on the blackboard site.)

**Note: Syllabus may evolve over the course of the term.**

- Check announcements portion of 95-764 Blackboard site at least once per week, preferably the Friday before class.
- For your review, the Carnegie Mellon University Policy on Cheating and Plagiarism is located at
  
  [http://www.cmu.edu/policies/documents/Cheating.html](http://www.cmu.edu/policies/documents/Cheating.html)

- For your review, the Carnegie Mellon University Graduate Academic Disciplinary Actions Overview is located at
  
  [http://www.cmu.edu/policies/documents/GradDisc.html](http://www.cmu.edu/policies/documents/GradDisc.html)

- For your review, the Statement on Academic Integrity is located within the Academic Standards, Policies and
Tentative Course Outline:  [Subject to change]

<table>
<thead>
<tr>
<th>Week/Date</th>
<th>Coverage, Readings, Quizzes, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 2: January 24</td>
<td><strong>CASE: Kraft Foods, Inc Protecting Employee Data</strong>&lt;br&gt;<strong>Required Reading:</strong>&lt;br&gt;Pages 1-24 in the required text&lt;br&gt;Course Syllabus (on BlackBoard site) – read in its entirety&lt;br&gt;<strong>Required Viewing:</strong>&lt;br&gt;View 12 minute movie (73MB) “Warriors of the Net”: <a href="http://www.warriorsofthe.net/">http://www.warriorsofthe.net/</a>&lt;br&gt;<strong>Quiz #1</strong></td>
</tr>
<tr>
<td>Week 3: January 31</td>
<td><strong>CASE: Advo, Inc.: Integrating IT and Physical Security</strong>&lt;br&gt;<strong>Required Reading:</strong>&lt;br&gt;Pages 25- 60 in the required text&lt;br&gt;<strong>Quiz #2</strong></td>
</tr>
<tr>
<td>Week 4: February 7</td>
<td><strong>CASE: Yale New Haven Center for Emergency Preparedness and Disaster Response: Contingency Planning</strong>&lt;br&gt;<strong>Required Reading:</strong>&lt;br&gt;Pages 61-88 in the required text&lt;br&gt;<strong>Quiz #3</strong></td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
|                     | **Required Reading:**
|                     | Pages 115-160 in the required text
|                     | **Quiz #4**
| Week 6: February 21 | CASE: Aetna: Developing and Implementing a Successful Information Security Awareness Program |
|                     | **Required Reading:**
|                     | Pages 184-207 in the required text
|                     | **Quiz #5**
|                     | **CISO Paper due**
| Week 7: February 28 | SPECIAL GUEST LECTURE – Mr. William Shore, Manager of Security, Software Engineering Institute, Carnegie Mellon University |
|                     | Students that attend the *entire* lecture will be awarded 1) 10 points for Quiz (otherwise 0 points), 2) 5 points for their Case Study question presentation grade (otherwise 0 points), and 3) 5 points for their Case Study question narrative grade (otherwise 0 points).
|                     | **PLEASE NOTE –**
|                     | READ the FBI Case Study with respect to what the MISSION of the FBI Computer Analysis and Response Team is prior to Feb. 28th [CASE: FBI New Haven Field Office – Computer Analysis and Response Team: Tracking a Computer Intruder] starts on page 161 in the Required text.]

**LEARNING OBJECTIVES**

Learning Objectives for “Special Topics: Information Assurance and Security” [95-764]:

Upon successful completion of this course, the student should be able to

- define key, basic information assurance and information security concepts
- describe the Information Security Model as it relates to the information properties, information states, and security measures dimensions of security
- discuss concepts involved in protecting employee data, including cross border concerns
- describe an example of the integration of IT and physical security
- discuss security and other considerations relevant to contingency planning for emergency preparedness and disaster response
describe the elements of the development and implementation of a successful information security awareness program

describe several (US) federal government regulations related to requirements for information security

enumerate, for each of the following 5 areas addressed by case studies
  - Data privacy (including cross border concerns)
  - Physical security (and its tie to cybersecurity)
  - Contingency planning
  - Risk management/risk assessment/legal issues/governance
  - Security awareness, education and training

questions the Chief Information Security Officer (CISO) should ask of or examples of information the CISO would need from each of the following 4 senior managers

  - Chief Information Officer
  - Chief Operating Officer
  - Chief Financial Officer
  - Chief Legal Officer