Georgia State University  
Department of Computer Information Systems  
Sample Course Syllabus -- Check with your instructor for the syllabus for your course

CIS 4680 – Introduction to Security and Privacy of Information and Information Systems

This syllabus provides a general guideline for the conduct of the course; however deviations may be necessary.

Prerequisites: CIS 2010 (or permission of the instructor)


Schedule of Topics: http://www3.cis.gsu.edu/cstucke/cis4680/spring2010/CIS4680schedule.html (changes from semester to semester...)

Course Description

The purpose of this course is to introduce the business student to the rapidly evolving and critical international arenas of Privacy, Information Security, and Critical Infrastructure. This course is designed to develop knowledge and skills for security of information and information systems within organizations. It focuses on concepts and methods associated with security across several systems platforms, including internal and Internet-facing systems. The course utilizes a world view to examine critical infrastructure concepts as well as techniques for assessing risk associated with accidental and intentional breaches of security in a global network. It introduces the associated issues of ethical uses of information and of privacy considerations.

Course Objectives

Upon successful completion of this course, students will develop a broad appreciation for and a basic understanding of

- The overall framework of information security and privacy
- The range of stakeholders concerned about information security and privacy
- The relationship between ethics, privacy, and information decisions
- The nature of common information hazards
- The basic operation and limitations of common information and system safeguards
- The milieu of laws, codes of practice, and standards that form the context for information security and privacy
- The national critical infrastructure components

Based on this understanding, students will develop qualifications to

1. Recognize and analyze primary threat scenarios of potential vulnerabilities for selected ...
Identify typical safeguards for computer-based information assets
3. Understand and explain organizational policies for information security and privacy
4. Envision limited risk analyses and potential organizational responses
5. Identify appropriate organizational structure within selected typical circumstances

The organizing principle for the course is drawn toward the attainment of these five qualifications.

Class Policies:

Prerequisites are strictly enforced. Students failing to complete a prerequisite with a grade of "C" or higher will be administratively withdrawn from the course in which they are in violation with a loss of tuition fees. There are no exceptions.

Students are expected to attend all classes and group meetings (whether online or in person), except when precluded by emergencies, religious holidays or bona fide extenuating circumstances.

Students who, for non-academic reasons beyond their control, are unable to meet the full requirements of the course should notify the instructor. Incompletes may be given if a student has ONE AND ONLY ONE outstanding assignment.

Please see http://www.gsu.edu/es/20399.html for details regarding withdrawals.

Spirited class participation is encouraged and informed discussion in class is expected. This requires completing readings and assignments before class.

Unless specifically stated by the instructor, all exams and lab assignments are to be completed by the student alone.

Within group collaboration is allowed on project work. Collaboration between project groups will be considered cheating unless specifically allowed by an instructor.

Copy work from the Internet without a proper reference will be considered plagiarism and subject to disciplinary action as delineated in the Student Handbook.

Any non-authorized collaboration will be considered cheating and the student(s) involved will have an Academic Dishonesty charge completed by the instructor and placed on file in the Dean’s office and the CIS Department. All instructors regardless of the type of assignment will apply this Academic Dishonesty policy equally to all students. See excerpt from the Student Handbook below.

Academic Honesty

(Abstracted from GSU’s Student Handbook Student Code of Conduct “Policy on Academic Honesty and Procedures for Resolving Matters of Academic Honesty” - http://www2.gsu.edu/~wwdos/codeofconduct.html )

As members of the academic community, students are expected to recognize and uphold standards
of intellectual and academic integrity. The University assumes as a basic and minimum standard of conduct in academic matters that students be honest and that they submit for credit only the products of their own efforts. Both the ideals of scholarship and the need for fairness require that all dishonest work be rejected as a basis for academic credit. They also require that students refrain from any and all forms of dishonorable or unethical conduct related to their academic work.

Students are expected to discuss with faculty the expectations regarding course assignments and standards of conduct. Here are some examples and definitions that clarify the standards by which academic honesty and academically honorable conduct are judged at GSU.

_Plagiarism_. Plagiarism is presenting another person’s work as one’s own. Plagiarism includes any paraphrasing or summarizing of the works of another person without acknowledgment, including the submitting of another student’s work as one’s own. Plagiarism frequently involves a failure to acknowledge in the text, notes, or footnotes the quotation of the paragraphs, sentences, or even a few phrases written or spoken by someone else. The submission of research or completed papers or projects by someone else is plagiarism, as is the unacknowledged use of research sources gathered by someone else when that use is specifically forbidden by the faculty member. Failure to indicate the extent and nature of one’s reliance on other sources is also a form of plagiarism. Failure to indicate the extent and nature of one’s reliance on other sources is also a form of plagiarism. Any work, in whole or part, taken from the Internet or other computer based resource without properly referencing the source (for example, the URL) is considered plagiarism. A complete reference is required in order that all parties may locate and view the original source. Finally, there may be forms of plagiarism that are unique to an individual discipline or course, examples of which should be provided in advance by the faculty member. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly or creative indebtedness, and the consequences of violating this responsibility.

_Cheating on Examinations_. Cheating on examinations involves giving or receiving unauthorized help before, during, or after an examination. Examples of unauthorized help include the use of notes, texts, or “crib sheets” during an examination (unless specifically approved by the faculty member), or sharing information with another student during an examination (unless specifically approved by the faculty member). Other examples include intentionally allowing another student to view one’s own examination and collaboration before or after an examination if such collaboration is specifically forbidden by the faculty member.

_Unauthorized Collaboration_. Submission for academic credit of a work product, or a part thereof, represented as its being one’s own effort, which has been developed in substantial collaboration with assistance from another person or source, or computer honesty. It is also a violation of academic honesty knowingly to provide such assistance. Collaborative work specifically authorized by a faculty member is allowed.

_Assignments & Grading_

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Labs and Cases</td>
<td>20%</td>
</tr>
<tr>
<td>Security issues white paper:</td>
<td>20%</td>
</tr>
<tr>
<td>Exams:</td>
<td>40%</td>
</tr>
<tr>
<td>Class Participation:</td>
<td>20%</td>
</tr>
<tr>
<td>Total:</td>
<td>100%</td>
</tr>
</tbody>
</table>
Refer to the **class schedule** for the due dates and timing of examinations. Any assignments turned in late are subject to a 10% per day penalty.

**Special Considerations**
The course web site will be used as a repository for examples of course paper problems, model solutions, examples of projects, and further required course material that arises during the class. Students must arrange for their own access to the World Wide Web (Internet access is available free in the GSU labs). All student work submitted in fulfillment of course requirements is deemed to be granted in the public domain (copyright-free) for the purposes of use as instructional material or examples of student work in future courses. The course syllabus provides a general plan for the course. Deviations may be necessary.

**Lab and Case Preparation**
Students will form teams of 3 individuals and prepare one assigned policy lab or case presentation. There will be policy labs in which student teams select, critique and expand organizational information security and privacy policies. There are several discussion cases during the class. Student teams will be assigned to present cases. Teams will focus on why events are unfolding as described in the case; and alternatives, possible actions that IT management might take or recommend in such settings and the potential outcomes of these actions.

**Security Issues White Paper**
Choose an area of information security management, ethics, or privacy that interests you and research it through the electronic media and the library. Discuss the topic with your instructor early in the term for counsel and approval. Write about a ten page (or more), single-spaced paper on the subject. A bibliography of references must be included.

*Your goal should be to address a managerially significant issue and to propose an action plan to address it.* Examples of interesting topics might be: “Security Aspects of Peer-to-Peer Computing (or IM or Cloud Computing)”, “The Impact of Wireless on Corporate (or Home) Networks”.

**Deliverable:** One ten-fifteen page plus term paper in electronic form and a PowerPoint presentation to be used when you deliver your paper in session.

**Team Assignment and Peer Appraisal**
All course assignments and lab exercises will be team-executed in groups. These groups should function as a self-managed team and adopt the rules and practices of this organizational work structure. Participation in the course assignments/lab exercises should be relatively equal among the group members, with each member monitoring both one’s own level and quality of participation and that of the other members of the group.

Consonant with the concepts and principles of self-managed teams, peer appraisals will be part of the overall grading/evaluation of individual performance. In the best managed teams, consensus on the relative contributions of each of the team members will be derived through assessment of

<table>
<thead>
<tr>
<th>Grade</th>
<th>A+</th>
<th>A</th>
<th>A-</th>
<th>B+</th>
<th>B</th>
<th>B-</th>
<th>C+</th>
<th>C</th>
<th>C-</th>
<th>D</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Points</td>
<td>97.0 - 100</td>
<td>93.0 - 96.9</td>
<td>90.0 - 92.9</td>
<td>87.0 - 89.9</td>
<td>83.0 - 86.9</td>
<td>80.0 - 82.9</td>
<td>77.0 - 79.9</td>
<td>73.0 - 76.9</td>
<td>70.0 - 72.9</td>
<td>60.0 - 69.9</td>
<td>Below 60.0</td>
</tr>
</tbody>
</table>
documented facts and records, evaluation of team output, and evaluation of team processes.

Please see [http://www3.cis.gsu.edu/cstucke/common/PeerEvaluation.htm](http://www3.cis.gsu.edu/cstucke/common/PeerEvaluation.htm) for more details. The average peer evaluation score for a team member is multiplied by the team project grade to get the individual team member grade.

The instructor is appreciative to Dr. Ram Sriram, Dr. Detmar Straub, Dr. Richard Baskerville, and others for allowing their materials to be adapted and used in this course. Also, the instructor thanks our speakers who enrich our course with their substantial experience and knowledge.