Georgia State University
Department of Computer Information Systems

Course Syllabus

ACCT 8680 / CIS 8080
(CRN 81334/82858)
Security and Privacy of Information and Information Systems
Fall 2011

Professor
Name Richard Baskerville
Office RCB Building, 35 Broad Street, 919
Office Hours Tuesdays, 3.00 pm – 5.00 pm, or by appointment
Office Phone (404) 413-7362
Office Fax (404) 413-7394
Email baskerville@acm.org

Venues
Tuesdays, 7.15 – 9.45 pm, 331ALC
Some sessions will be conducted online (see course schedule).

Prerequisites
None. CSP: 1, 2, 3, 4, 5, 6, 7, 8.

Required Materials
Course Web Site:  http://cis.gsu.edu/~rbaskerv/cis8080/index.html

Most course readings will be available via GSU library subscriptions or from the course web site. The exceptions are the four HBR case studies that must be downloaded directly from HBR (for a fee payable to HBR at time of downloading). The download link for these cases is:

http://cb.hbsp.harvard.edu/cb/access/9790160

See “Readings” below for a complete list of required reading material.

Catalog Description
This course is designed to develop knowledge and skills for the management and assurance of security of information and information systems in technology-enabled environments. It focuses on concepts and methods associated with planning, designing, implementing, managing, and auditing security at all levels on different platforms, including worldwide networks for e-business. The course presents techniques for assessing risk associated with accidental and intentional breaches of security and covers the associated issues of ethical uses of information and privacy considerations.
Course Objectives

Students completing this course will be capable of:

1. distinguishing the relationships of various information systems elements with threats and security features that protect the elements from these threats, viz.,
   a. applying a TFO Model to an organizational setting,
   b. using a comprehensive IT Threats Framework to develop scenarios for an organizational setting,
   c. using an IT Safeguards Framework to develop alternatives for IT security controls,
2. analyzing and evaluating the ethics of information development and use, viz.,
   a. incorporating Privacy Law into security planning,
   b. incorporating public accounting legal requirements (e.g., SARBOX) into security planning,
3. planning, designing, and implementing IT security, viz.,
   a. organizing and planning IT Risk Management operations,
   b. organizing the IT security function,
   c. adapting an organizational IT security methodology,
   d. constructing organizational policies,
4. auditing IT security, viz.,
   a. applying security standards (e.g., COBIT) to an organizational setting,
   b. determining organizational compliance with security standards, privacy laws, and public disclosure laws.

Special Considerations

The course web site will be used as a repository for further required course material that arises during the class. Three meetings are planned as online venues. Students must arrange for their own access to the World Wide Web (Internet access is available free in the GSU labs) and must establish their access capability to WebCT and Elluminate live prior to these meetings. 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. Constructive assessment of this course by students plays an indispensable role in shaping education at Georgia State. Upon completing the course, students are asked to take the time to fill out the online course evaluation. The course syllabus provides a general plan for the course. Deviations may be necessary.

Method of Instruction

Classroom sessions will regard the same topics as the readings assignments, but seek further depth through discovery learning. It is essential that students read the assigned material before coming to class. Instruction will follow these three approaches: (1) topic discussion of course concepts, (2) discussion of cases that will allow us to apply knowledge of information security concepts to actual business settings, and (3) class activities that apply these concepts to simulated business situations. Preparation is essential and all students are required to have read, and be prepared to discuss critically, the readings assigned. Individuals may be “cold called” to introduce an article or to initiate discussion. In assigning the participation grade, both class attendance and the quality of oral contributions during class discussions will be considered.
Class Attendance Policy
Roll will not be taken on a regular basis. It is the student’s responsibility to attend class, obtain assignments, and turn in work on time. Absence from class does not relieve you of any of these responsibilities. One absence will be considered excused if it is due to an emergency, a religious holiday, or some other extenuating circumstance. Please notify the instructor in advance if possible. Unless an absence is excused, students will NOT be allowed to make up missed work. A low-score drop mechanism will automatically satisfy one absence, excused or unexcused, from the in-class quizzes. Further absences may impact a student’s grade due to missed in-class activities.

Flicker and Noise Distractions
By continued enrollment in this class, students agree to practice a “click-free”, “flicker-free” and “noise-free” environment for fellow students in this classroom. Students agree that mobile devices such as telephones, pdas, Blackberries, etc. will be silenced and unused during class. Students agree to forebear from the use of computers during the class for email, web-surfing, gaming, etc.

Withdrawals
Students who withdraw before the midpoint will receive a grade of W. Students withdrawing after this date will receive a grade of WF unless a hardship authorization is obtained from the Dean of Students. For the exact midpoint date see http://calendar.gsu.edu/calendar.

Incompletes
A grade of I will be given only in exceptional circumstances. A student must have completed all but one of the requirements of the course in order to be eligible to receive a grade of I.

Assessment
Learning objectives will be assessed by both individual and group performance through the following course features:

Discussions
The course will include in-class discussions of five cases: (1) Secom, (2) ChoicePoint, (3) CareGroup (4) TJX and (5) Leih’s retailer. Students will have individual opportunities to contribute thoughtful and critical oral observations during class discussions focused on the course objectives. There will be readings assigned for most class meetings. Students will have opportunities during the semester to introduce and comment on these readings during in-class discussions. An email group server provides opportunities for discussions outside of class meeting times.

Team Activities
Four in-class team activities will be organized: (1) Threat scenarios, (2) Threat news reports, (3) Safeguards tradeshow, (4) Methodology bends. Assessment of performance is generally based on the quality of the deliverables in each activity. In some cases, these activities will be competitive, and small amounts of “bonus” credit may be awarded to winning teams. These activities are further described in the activity descriptions distributed in advance of the activities.
Students will form self-managing teams for the purpose of completing team activities. Each team is expected to persist through the course. Peer appraisals will be part of the overall grading/evaluation of individual performance. Consensus on the relative contributions of each of the team members will be derived through assessment of documented facts and records, evaluation of team output, and evaluation of team processes. Unless team members inform the instructor in writing to the contrary, the assumption will be that each team member contributed equally to the assessed products of the team.

**Quizzes**
There will be two short objective quizzes that assess familiarity with the principles and general organization of two examples of security management frameworks: (1) CobiT, and (2) Octave. Students will actively participate in the construction and evaluation of these quizzes.

**Short Paper**
Each student will prepare an essay that compares the ChoicePoint case (discussed during the course) with the recent Sony data breach (not discussed during the course) from a perspective of the ethical reasoning in security and privacy of information and information systems. The paper must demonstrate the student’s ability to research a case, analyze data, synthesize data from different sources, and to compare and to evaluate distinct cases with a clear train of argumentation and ethical reasoning using the perspective required. Any and all conclusions must be clearly stated. To insure research originality, students are strongly encouraged to seek information beyond web pages, and from at least one original source (such as an interview with an authority on the subject). The paper must be submitted both in paper and electronic form (as a Microsoft Word Document), no longer than 2000 words, and include citations and full references to all direct sources (in APA format).

**Short Paper Discussion**
Each student will prepare a brief (e.g. three-minute) presentation of their essay that features its point-counterpoint relationship to at least one other student short paper. This discussion should authoritatively (i.e. by citing references) compare and contrast the central arguments and conclusions of their paper with at least one other student short paper. PowerPoint may not be used. Students may or may not be called on to present during class at the discretion of the instructor. Order of progression will be determined in a bidding session and draft papers exchanged one week before the discussion.

**Grading Policy**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Points Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case and readings discussions</td>
<td>400</td>
</tr>
<tr>
<td>Team activities</td>
<td>300</td>
</tr>
<tr>
<td>Quizzes</td>
<td>100</td>
</tr>
<tr>
<td>Short paper</td>
<td>150</td>
</tr>
<tr>
<td>Short paper discussion</td>
<td>50</td>
</tr>
<tr>
<td>Total</td>
<td>1000</td>
</tr>
<tr>
<td>Letter Grade</td>
<td>Percentage Range</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>A+</td>
<td>&gt;96%</td>
</tr>
<tr>
<td>A</td>
<td>90% - 96%</td>
</tr>
<tr>
<td>A-</td>
<td>87% - 89%</td>
</tr>
<tr>
<td>B+</td>
<td>83% - 86%</td>
</tr>
<tr>
<td>B</td>
<td>80% - 82%</td>
</tr>
<tr>
<td>B-</td>
<td>77% - 79%</td>
</tr>
<tr>
<td>C+</td>
<td>73% - 76%</td>
</tr>
<tr>
<td>C</td>
<td>70% - 72%</td>
</tr>
<tr>
<td>C-</td>
<td>67% - 69%</td>
</tr>
<tr>
<td>D</td>
<td>60% - 66%</td>
</tr>
<tr>
<td>F</td>
<td>0% - 59%</td>
</tr>
</tbody>
</table>

**Readings**

Note: Accessing some of these resources may only be completed from an on-campus computer or through a VPN connection from off-campus. An on-campus IP address is usually required. For more information see “Connecting to the Network from Home (VPN - Virtual Private Network)” at [http://www.gsu.edu/help/25697.html](http://www.gsu.edu/help/25697.html)


**Academic Honesty**


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.* 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.

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.
<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Lesson Topic</th>
<th>Meeting Activities</th>
<th>Deliverables</th>
<th>Reading Discussions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>23-Aug</td>
<td>TFO &amp; Incident centered security management</td>
<td>Team Organization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>30-Aug</td>
<td>Organizational context of IT Security (COBIT)</td>
<td>Management of IS Security Case</td>
<td>1. IT Resources: (IT Governance Institute, 2007, read pp. 5-28) 2. Secom Case: (McFarlan et al., 2008)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Visitor: *Karen MacDonald – Biz Librarian</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>6-Sep</td>
<td>IT Threats Framework</td>
<td>Threats scenarios for Jashopper</td>
<td>1. Risk Mgmt: (Tsouh et al., 2006) 2. IT Threats Framework: (Im &amp; Baskerville, 2005)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Visitor: Chase Whitaker, Matt Edman and Josh Hubbard, HCI Auditing</td>
<td>News Reports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>20-Sep</td>
<td>COBIT Controls</td>
<td>CareGroup Case Discussion</td>
<td>Quiz: COBIT</td>
<td>1. CareGroup Case (McFarlan &amp; Austin, 2005) 2. COBIT and 17799: (von Solms, 2005)</td>
</tr>
<tr>
<td>6</td>
<td>27-Sep</td>
<td>Hacking and its prevention (Online Lesson)</td>
<td>Online Lesson: Hacker Toolboxes</td>
<td>1. Hacking: (Baskerville, 2005) 2. and (Young et al., 2007) 3. Phishing: (Herzberg, 2009)</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>18-Oct</td>
<td>Regulation: SARBOX, HIPPA, etc.</td>
<td>Safeguards Trade Show</td>
<td>Safeguards booth</td>
<td>1. Regulation Risk: (Berghel, 2005), 2. SOX 404 compliance (Wallace et al., 2011)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guest Professor: Carl Stucke</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Visitor: Tammy Clark GSU CISO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Week</td>
<td>Date</td>
<td>Lesson Topic</td>
<td>Meeting Activities</td>
<td>Deliverables</td>
<td>Reading Discussions</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>-------------------------------------</td>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
2. and Method: (Alberts & Dorofee, 2001)  
3. Method Framework (Siponen et al., 2006, read pp. 1-13) |
| 12   | 8-Nov  | IT Security functions and policy (ISO 27001)  | TJX Case Discussion     |                                                                               | 1. TJX Case (Xu et al., 2008)  
2. TJX Case Audit (Berg et al., 2008) |
| 13   | 15-Nov | IT Audit & Disclosure               | IT Project Management Audit Case  
Visitor: Eric Brothers, Advisory Services, E&Y  
Draft Short Paper Hard Deadline  
Discussion Bidding                   | 1. Forensics: (Luoma, 2006)  
2. Leih’s Case (Leih, 2006, read pp. 20-28)                   |
|      | 22-Nov | Thanksgiving Holiday                |                          |                                                                               |                                                                                     |
| 14   | 29-Nov | Short Research Paper Presentations  |                          | Short Paper & Discussion Deadline                                            |                                                                                     |