Georgia State University
Department of Computer Information Systems

Course Syllabus

CIS 8080 / ACCT 8680

(CRN 19394 BA)

Information Systems Security and Privacy

Spring MM1 2019
(Version 1.5 15 Jan 2019)

Instructor

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

Teaching Assistant

Name	Indeah Vincent
Location	RCB Buckhead Center
Office Hours	Mondays, 3.00 pm – 5.00 pm, or by appointment
Email	ivincent3@student.gsu.edu

Visiting Instructor

Name	Pengcheng Wang
Location	RCB 910
Office Hours	By appointment
Email	pwang12@gsu.edu

Venues

Wednesdays, 5.30 – 9.45 pm Buckhead Center, Room 601

Prerequisites

None.

Required Materials

Course Web Site: http://cis.gsu.edu/rbaskerville/cis8080/

Course readings consist of published research journal articles, published cases, and certain online reports and publications. These are generally available via study.net or downloadable directly from the source without charge. No textbook is required.

Study.net course web site: http://www.study.net/r_mat.asp?crs_id=30138485

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. constructing organizational policies,
4. auditing IT security, viz.,
    a. applying security standards (e.g., ISO or 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. The main online tool for group projects is iCollege. 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 iCollege. 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 principles and concepts, (2) discussion of cases that will 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

Students are not permitted to miss classes without prior arrangements. In cases of absence due to emergency, contact the instructor as soon as possible. It is the student's responsibility to attend class, obtain assignments, and turn in work on time. Absence from class does not relieve students of these responsibilities. Unless an absence is excused, students will NOT be allowed to make up missed work.

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 will be silenced and unused except for in-class purposes. Students agree to forebear from the use of email, web-surfing, gaming, social-networking 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:

Case Research and Presentation
The course will include in-class discussions of assigned readings and six cases: (1) BCIA Airport, (2) Apple, (3) Enterall Infosec, (4) Intel, (5) Titan, and (6) Target. All students should

prepare for discussing these cases not only by reading the case texts, but the preparation readings for the session. Assigned student panel groups will provide further research and offer an expert discussion of each case and afterwards an open discussion by all students will provide individual opportunities to contribute thoughtful and critical oral observations during class discussions focused on the course objectives and anchored to the course readings assigned for most class meetings.

In addition to the in-class panel activity, the group must submit its PowerPoint deck for grading. To insure research originality, groups are required to seek information from refereed literature to back its claims. The work must be authoritative, including citations and full references to all direct sources.

Grading: Pass/Fail (One retry allowed)

Discussions

Students will have opportunities during the semester to comment on the course readings during in-class discussions. An email group server provides opportunities for discussions outside of class meeting times.

Grading: Assessed weekly and curved.

Group Activities

Four in-class group activities will be organized: (1) Threat scenarios, (2) Threat news reports, (3) Ethical hacking demonstration, and (4) Agility Tournament. Assessment of performance is generally based on the quality of the deliverables in each activity and student evaluations of deliverables may be components of this assessment. These activities will be competitive and are further detailed in the activity descriptions distributed before the activities.

Students will form self-managing groups for the purpose of completing group activities. Each group is expected to persist through the course. Peer appraisals may be part of the overall grading/evaluation of individual performance. Consensus on the relative contributions of each of the group members will be derived through assessment of documented facts and records, evaluation of group output, and evaluation of group processes. Unless group members inform the instructor in writing to the contrary, the assumption will be that each group member contributed equally to the assessed products of the group.

Grading: Curved. Up to 100 points each. No retakes, instead the lowest grade drops.

Quizzes

There will be six short, objective, multiple-choice quizzes given at the beginning of class that assess familiarity with the class preparation materials (videos, readings, cases, etc). Students must be physically present in the room to participate.

Grading: Curved. No makeups, instead lowest grade drops.

Tradeshow Participation
Each group will prepare a class tradeshow entry that critically explains and assesses an approved commercially available information security product. The entry must demonstrate the students' ability to research a technical problem and its solutions, analyze data, synthesize data from different sources, and to compare and to evaluate distinct solution products with a clear train of fact-based argumentation. Any and all conclusions and recommendations must be clearly stated.

To insure research originality, students are required to seek information beyond web pages, and from refereed literature. The work must be authoritative, including citations and full references to all direct sources. Student group evaluations of tradeshow entries are components of this assessment.

Grading: Curved.

Grading Policy

Activity	Points Available
Case research and presentation	200
Weekly contributions in class and in online discussions	300
Group activities	300
Quizzes	100
Tradeshow	100
Total	1000

Letter Grade	Percentage Range	Point Range
A+	>98%	>980
A	95% - 98%	950 - 980
A-	91% - 94%	910 - 949
B+	87% - 90%	870 - 909
B	83% - 86%	830 - 869
B-	77% - 82%	770 - 829
C+	73% - 76%	730 - 769
C	70% - 72%	700 - 729
C-	67% - 69%	670 - 699
D	60% - 66%	600 - 669
F	0% - 59%	0 - 599

Readings

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

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management, 35*(6), 717-723.

Anderson, R. (2018). Making security sustainable. *Communications of the ACM, 61*(3), 24-26.

Bartnes, M., Moe, N. B., & Heegaard, P. E. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers & Security, 61*(Supplement C), 32-45.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response. *Information & Management, 51*(1), 138-151.

Berghel, H. (2005). The two sides of ROI. *Association for Computing Machinery. Communications of the ACM, 48*(4), 15-20.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Carnegie Mellon University Software Engineering Institute.

Chandrasekhar, R. (2013). *Intel Corp. - Bring Your Own Device* (No. W13035). London, Ontario: Richard Ivey School of Business, The University of Western Ontario

Chong-Leng Goh, J., Yun Zuo, M., & Pan, S. L. (2016). Achieving the delicate balance between risks & outcomes in a large-scale IT project – a case study on BCIA’s airport security system. *Journal of Information Technology Teaching Cases, 6*(1), 36-44.

Cook, A., Janicke, H., Smith, R., & Maglaras, L. (2017). The industrial control system cyber defence triage process. *Computers & Security, 70*(Supplement C), 467-481.

Genkin, D., Pachmanov, L., Pipman, I., Shamir, A., & Tromer, E. (2016). Physical key extraction attacks on PCs. *Communications of the ACM, 59*(6), 70-79.

Genkin, D., Papadopoulos, D., & Papamanthou, C. (2018). Privacy in decentralized cryptocurrencies. *Communications of the ACM, 61*(6), 78-88.

ISO/IEC. (2013a). *ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements* (International Standard No. ISO/IEC 27001:2013). Geneva: International Standards Organization

ISO/IEC. (2013b). *ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management* (International Standard No. ISO/IEC 27002:2013). Geneva: International Standards Organization

Khansa, L., & Zobel, C. W. (2014). Assessing innovations in cloud security. *Journal of Computer Information Systems, 54*(3), 45-56.

Kugler, L. (2015). Online Privacy: Regional Differences. *Communications of the ACM, 58*(2), 18-20.

Lynton, M., & Ignatius, A. (2015). “They Burned the House Down”. *Harvard Business Review, 93*(7/8), 106-113.

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons, 59*(3), 257-266.

McGee, H., Hsiêh, N.-H., & Mcara, S. (2016). *Apple: Privacy vs. Safety?* Cambridge, Mass: Harvard Business School Case 9-316-069)

McLaughlin, M.-D. J., Cram, W. A., & Gogan, J. L. (2015). A high performance computing cluster under attack: the Titan incident. *Journal of Information Technology Teaching Cases, 5*(1), 1-7.

NIST. (2012). *Guide for Conducting Risk Assessments* (No. SP800-30). Gaithersburg, MD: U.S. Department of Commerce National Institute of Standards and Technology http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

NIST. (2014). *Framework for Improving Critical Infrastructure Cybersecurity*: National Institute of Standards and Technology http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf)

Osborn, E., & Simpson, A. (2017). On small-scale IT users' system architectures and cyber security: A UK case study. *Computers & Security, 70*(Supplement C), 27-50.

Pfleeger, S. L., & Cunningham, R. K. (2010). Why Measuring Security Is Hard. *Security & Privacy, IEEE, 8*(4), 46-54.

Preibusch, S. (2015). Privacy Behaviors After Snowden. *Communications of the ACM, 58*(5), 48-55.

Rees, J., & Allen, J. (2008). The State of Risk Assessment Practices in Information Security: An Exploratory Investigation. *Journal of Organizational Computing and Electronic Commerce, 18*(4), 255-277.

Savage, N. (2016). The Key to Privacy. *Communications of the ACM, 59*(6), 12-14.

Scofield, M. (2016). Benefiting from the NIST Cybersecurity Framework. *Information Management, 50*(2), 25.

Trapero, R., Modic, J., Stopar, M., Taha, A., & Suri, N. (2017). A novel approach to manage cloud security SLA incidents. *Future Generation Computer Systems, 72*(Supplement C), 193-205.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2006). Formulating information systems risk management strategies through cultural theory. *Information Management & Computer Security, 14*(3), 198-217.

Verizon Risk Team. (2017). 2017 Data Breach Investigations Report [Electronic Version], from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Verma, V., Pathak, A. A., Bathini, D. R., & Pereira, A. (2014). *Enterall Infosec Solutions: Growing an Ethical Hacking Business*. London, Ontario: Richard Ivey School of Business University of Western Ontario W14608 Version 2014-12-09)

Wallace, L., Lin, H., & Cefaratti, M. (2011). Information Security and Sarbanes-Oxley Compliance: An Exploratory Study. *Journal of Information Systems, 25*(1), 185-211.

Werlinger, R., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security, 18*(1), 26-42.

Winnefeld Jr, J. A., Kirchhoff, C., & Upton, D. M. (2015). Cybersecurity's Human Factor: Lessons from the Pentagon. *Harvard Business Review, 93*(9), 86-95.

Academic Honesty

Students are expected to know and understand Section 2 of The Policy on Academic Honesty found in the Academic Conduct Policies and Procedures section of the GSU Student Code of Conduct. This section provides definitions and examples of academic dishonesty. These definitions are considered part of this syllabus and will apply in this course. See http://codeofconduct.gsu.edu/ for details.

Course Schedule (Subject to Change)

Meet	Date	Part	Lesson Topic	Deliverables	Preparation Reading
1	9-Jan		**Course Intro**		
		1	Principles Discussion: TFO & Incident centered security management		(Baskerville et al., 2014)
		2	Confirmed Visitor: Dan Lê, MLIS, MBA Business & Science Librarian		Scholarly vs. Popular Articles https://www.youtube.com/watch?v=Ud0U-NWuIj8 How to Find Scholarly Articles https://www.youtube.com/watch?v=AnErBiXMLx8
		3	Syllabus & Plan		
		4	Group Activities: Group News Organization		
2	16-Jan		**Organization Assets**		
		1	Principles Discussion: Assets: Organizational context of IT Security	Quiz #1	NIST Cybersecurity Framework (NIST, 2014; Scofield, 2016) NIST SP-800-30: (NIST, 2012, pp. 4-39) Safety: (Anderson, 2018)
		2	Case Discussion: Management of IS Security		BCIA Airport Case: (Chong-Leng Goh et al., 2016)
		3	Group Activity: Threats scenarios for BCIA Airport	Group scenarios & evaluations	Octave Scenarios (Caralli et al., 2007, p. 48-52)
3	23-Jan		**Threats**		
		1	Principles Discussion: IT Threats & Privacy	Quiz #2	Privacy: (Kugler, 2015; Preibusch, 2015) Hacking: (Lynton & Ignatius, 2015)
		2	Confirmed Visitor: Will Bracker, Cox Communications		
		3	Case Discussion: IT Threats		Apple: Privacy vs. Safety (McGee et al., 2016)
		4	Group Activity: IT Threats News Reports	News Report Script	Optional: Physical Attacks (Genkin et al., 2016). 2017 Data Breach Investigations Report (Verizon Risk Team, 2017)
4	30-Jan		**Controls & Safeguards**		

Meet	Date	Part	Lesson Topic	Deliverables	Preparation Reading
		1	Principles discussion: (1) Features: Control Safeguard Standards & Technologies (2) Encryption	Quiz #3	Cyber Defense: (Winnefeld Jr et al., 2015) Cloud Controls: (Khansa & Zobel, 2014) Diffie Helman: (Savage, 2016)
		2	Confirmed Visitor: Joshua Nelkin, Grant Thornton		
		3	Case Discussion: Protection Solutions		Enterall Infosec Solutions (Verma et al., 2014)
		4	Group activity: Ethical hacking preparation	Demonstration script	Optional: Privacy in Bitcoin: (Genkin et al., 2018) ISO 27001/27002 (ISO/IEC, 2013a, p. 1-9; 2013b, p. vi-8)
5	6-Feb		**Risk Management**		
		1	Principles discussion: IT Risk Management	Quiz #4	Risk Analysis: (Rees & Allen, 2008) Measuring Risk: (Pfleeger & Cunningham, 2010) Risk Mgmt: (Tsohou et al., 2006)
		2	Invited Visitor: TBA		
		3	Case: BYOD		Intel (Chandrasekhar, 2013)
		4	Group Activity: Ethical Hacking Demonstrations		Optional: Small-Scale CyberSecurity (Osborn & Simpson, 2017)
6	13-Feb		**Incident Response**		
		1	Principles discussion: Incident Response	Quiz #5	Incident Groups: (Ahmad et al., 2015) Diagnostics: (Werlinger et al., 2010) Triage (Cook et al., 2017)
		2	Confirmed Visitor: Priya Palaniappan, Damon Crumblin, RELX		
		3	Case: A CERT in action		Titan incident (McLaughlin et al., 2015)
		4	Group Activity: Agility Tournament		Optional: Incidents in the cloud (Trapero et al., 2017)
7	20-Feb		**Learning and Refining**		
		1	Principles discussion: Regulation & Audit	Quiz #6	Regulation Risk: (Berghel, 2005), SOX 404 compliance (Wallace et al., 2011) Training: (Bartnes et al., 2016)

Meet	Date	Part	Lesson Topic	Deliverables	Preparation Reading
		2	Confirmed Visitor: Gayathri Kunapuli, E&Y		
		3	Case: Reflections on an Incident		Target Ethics (Manworren et al., 2016)
		4	Group Activity: Tradeshow Prep		
8	27-Feb		Tradeshow		
		1	Tradeshow Setup		
		2	Invited Visitor: Peter Chronis, Turner		Chronis 2018, Chs 1-3
		3	Tradeshow	Entry Brochure	