UNIVERSITY OF DELAWARE
Department of Accounting & MIS
MISY 850 – Security and Control
Spring 2018

Instructor:	Dr. John D'Arcy	**Office:**	356 Purnell Hall
E-mail:	jdarcy@udel.edu	**Phone:**	302-831-1793
Personal Website:	http://sites.udel.edu/jdarcy/		

Office Hours:	Tuesday, 4:45 – 5:45 pm or by appointment
Class Sessions:	Tuesday, 6:00 – 9:00 pm in Lerner Hall Room 231
Course Webpage:	via Canvas at http://www1.udel.edu/canvas/index.html

Course Description: As enterprises become increasingly reliant on electronic media and communication, the protection of data and electronic infrastructure becomes critically important. Incidences of information security failures in commercial and noncommercial environments are increasing in number and severity. Hence, it is essential that enterprises continually develop and refine information security strategies that reflect the changing uses of information technology. The development of this strategy becomes even more important and challenging as organizations become participants in the global economy.

This course is a survey of topics in the realm of information security. It will consider many contemporary topics ranging from basic cybersecurity threats to cyber-warfare to information security ethics to legal and cultural differences between countries. The course emphasizes managerial decision making through analyzing information security problems and understanding effective solutions. The course will culminate in a research project in which students conduct a real-world information technology risk assessment using an organization of their choice.

Course Objectives: Upon completion of this course, students should be able to:

- Recognize key information security issues that require management attention and effort in a modern business enterprise.
- Explain the current information security threat posture, and demonstrate an awareness of the likely evolution of security threats, regulations, and countermeasures.
- Understand the basic concepts of information technology risk management, including the tools and techniques involved in a risk assessment.
- Discuss the technical and human aspects of information security.
- Know how ethical, legal, and privacy issues define the environment in which information technology is viewed.
- Appreciate the future trends and issues in information security, including the social, technical, and organizational implications.

Required Materials:
Harvard Business School Cases: A digital course pack containing 6 cases ($4.25 each). It can be purchased and directly downloaded from HBS publishers using the following link:
http://cb.hbsp.harvard.edu/cbmp/access/76690496

A number of additional readings and materials will be distributed by the instructor or made available for download on the Canvas site.

Description of Major Course Activities:

Assignment	Portion of Grade
Class Participation	15%
International Assignment	10%
Case Study Presentation	10%
IT Risk Assessment Project	25%
Homework and Case Assignments	40%

Class Participation (15% of your grade): Contributing to classroom discussions is a valuable method of enhancing both your learning and the learning of your classmates. During class, we will examine a variety of concepts and ideas that can be enriched through the communication of your thoughts, experiences, and opinions. Every student is expected to be prepared to discuss the assigned material for each class session. There will be a variety of opportunities for participation, including classroom-wide discussions and in-class, small group discussions. Participation grades will be awarded for the quality of the contributions, while simple attendance at class does not constitute effective participation. In the event of an absence, it is the student's responsibility to get any missed notes, important announcements, or changes in assignments. Also, please read the **Evaluation of Contributions to Class Discussion/Participation** section of this syllabus.

Homework and Case Assignments (40% of your grade): There will be regular homework and case assignments during the semester. Details regarding each homework assignment will be provided the week before its due date. The case assignments will consist of case study analyses in which students are required to read a particular case and respond to a series of questions provided by the instructor. Grades for the case assignments will be based on demonstrated understanding of the case materials and personal insights on the case topic and assigned questions. Your answers should incorporate relevant class discussions and assigned readings. Unless otherwise specified, all homework and case assignments must be completed individually and handed in to the instructor as a hard copy on the assigned due date. Students are encouraged to make an extra copy for themselves for class discussion. The format for all homework and case assignments is typed in English, with 1.5 spacing and 12 point font.

NOTE: NO CREDIT WILL BE GIVEN FOR LATE ASSIGNMENTS; IF YOU MUST MISS CLASS, THE ASSIGNMENT IS STILL DUE ON THE ASSIGNED DATE.

International Assignment (10% of your grade): Working in groups of two, students will select a country to focus on and conduct research on the areas of security, privacy, and control for that country. Students are free to focus on an array of security-related topics for their country of interest, as long as it relates to the objectives of the course. The deliverable for this assignment is a 3-5 page paper and students will be called upon, in an informal manner (i.e., no formal presentation to the class required), to discuss their findings with the class. The due date for this assignment is *March 20th*.

Case Study Presentation (10% of your grade): Over the course of the semester, we will be covering six case studies, each of which will be presented by a group of students. Each group will be expected to provide a synopsis of their assigned case, lead an interactive discussion that includes addressing the assigned questions, and summarize the class discussion. Grading for this assignment will be based on the following criteria: preparation, quality of case overview and summary, quality of interactive discussion, and visual aids. Each group will meet with the instructor at least one week prior to their case study presentation for additional instruction.

IT Risk Assessment Project (25% of your grade): Working in small groups, students will perform an information technology risk assessment using an organization of their choice. Students will use the NIST Special Publication 800-30 and other relevant sources as a guide to prepare a report for management indicating the risks and vulnerabilities specific to their organization. The report should include diagrams and a risk matrix chart to help explain the findings. The deliverables are a formal, 12-15 page report delivered to the instructor and a presentation to the class. Additional details will be provided in class.

Grading: The final letter grade for the course will follow the following scale:

A	93-100	B-	80-82.99	D	63-66.99
A-	90-92.99	C+	75-79.99	D-	60-62.99
B+	87-89.99	C	70-74.99	F	Below 60
B	83-86.99	D+	67-69.99		

Dishonest Behavior: Dishonest and/or unethical behavior will not be tolerated. Such behavior includes (but is not limited to) cheating, copying homework, and plagiarism. If it is determined that any assignment was not written solely by the student whose name appears on the paper, the grade will be zero for the assignment and the student(s) involved may receive an "F" for the class in addition to having the incident reported to the Office of Student Conduct. Students are expected to abide by the University's Academic Honesty Policy, which can be found online at http://www1.udel.edu/stuguide/17-18/code.html.

"All students must be honest and forthright in their academic studies. To falsify the results of one's research, to steal the words or ideas of another, to cheat on an assignment, or to allow or assist another to commit these acts corrupts the educational process. Students are expected to do their own work and neither give nor receive unauthorized assistance.

When a student includes their name on a group assignment, that student is verifying the authenticity of the entire work. Therefore, it is important to know how others in the group obtained the material they contributed. If a violation of the Academic Honesty Policy is determined, all members of the group will share responsibility, unless the identity of individuals involved in the dishonesty can be determined. In cases where a student claims no knowledge of or involvement with dishonesty in group work, it will be the responsibility of that student to demonstrate this lack of knowledge and involvement.

Any violation of this standard must be reported to the Office of Student Conduct. The faculty member, in consultation with a representative from the Office of Student Conduct, will decide under which option the incident is best filed and what specific academic penalty should be applied."

Evaluation of Contributions to Class Discussion/Participation:
Effective participation is characterized by:

- *Relevant* points rather than repetition of facts
- *Interpretation* and *integration* of points made previously
- Willingness to test new ideas
- Challenges/tests ideas presented by others
- Reflects thorough understanding of the facts related to the assignment

Effective participation is different from attentive note-taking and passive listening. Participation will be gauged and points (and consequently final grades for participation) will be assigned based on the following categories:

- Outstanding: Comments reflect thorough preparation. Comments provide major insight and direction for the class. Requires active participation. (93-100)
- Good: The student is thoroughly prepared. Requires at least frequent participation. (87-93)
- Adequate: Contributions reflect adequate preparation. Requires at least semi-frequent participation. (83-87)
- Non-participant: The person has said little or nothing in class. There is no basis for evaluation. This person has no effect on the quality of class discussion. (75-83, depending on attendance)
- Unsatisfactory: Contributions demonstrate inadequate preparation. In-class comments are isolated, obvious, and often confusing. This person wastes class time. (less than 75)

Limitations: The course plan presented in this syllabus and detailed in the attached schedule will be followed to the extent possible. However, it may be necessary to make changes in the form of additions, deletions, and/or modifications (e.g., changing due dates). Any changes will be announced in class with sufficient lead-time. It is each student's responsibility to be aware of all announcements made in class.

Final Comments: I believe everyone has the right to take the class without undue hardship deriving from conditions such as physical or learning disabilities. If you have any such condition, please notify me in the first week of class and I will strive to make the appropriate accommodations. Confidentiality will be maintained.

TENTATIVE COURSE SCHEDULE (updated 2/22/18)

Class	Date	Topics	Articles/Readings	Deliverables
1	Feb. 6	Course Overview and Introduction to Information Security	• The Myth of Secure Computing • The Darknet: A Quick Introduction for Business Leaders	
2	Feb. 13	Risk Management Framework Asset Identification and Valuation	• W&M: pp. 117-129; 133-144 • NIST: pp. 8-12	Data Breach Assignment due
3	Feb. 20	Risks, Threats, and Vulnerabilities	• W&M: pp. 40-73	
4	Feb. 27	Attack Types: External Case 1: Apple: Privacy vs. Safety?		Case 1 due
5	March 6	Attack Tool Demos Case 2: Flayton Electronics & When Hackers Turn to Blackmail	• Why Hospitals Are Perfect Targets for Ransomware	Case 2 due
6	March 13	Legal and Compliance Issues International Security Issues Case 3: Google in China	• Protecting Corporate Intellectual Property • The Looming Shadow of Illicit Trade on the Internet	Case 3 due
7	March 20	International Security Issues	• IS Misuse in the U.S. and Korea • In Privacy Law, It's the U.S. vs. the World	International Assignment due
	March 27	No Class – Spring Break Week		
8	April 3	Attack Types: Internal Case 4: Aetna Security Awareness Program	• Are You the Weakest Link? • Dark Side of IT • Do Millennials Believe in Data Security?	Case 4 due
9	April 10	Attack Types: Internal Footprinting and Social Engineering	• Footprinting Tools and Techniques • Cybersecurity's Human Factor: Lessons from the Pentagon • Case: Autopsy of a Data Breach	Preliminary IT Risk Project Matrix due
10	April 17	Network Security Technologies Case 5: Intel – Bring Your Own Device	• An Analysis of Firewall Rulebase Mismanagement Practices	Case 5 due
11	April 24	Emerging Issues: Mobile Security, Social Media, Cloud Computing, etc.	• What Every CEO Needs to Know About the Cloud • Physical and Information Security in the Age of the Wearable Device • Case: The Vulnerability Economy	
12	May 1	Business Continuity Planning Security and Personnel Case 6: Secom	• W&M: Chapter 11 • The Emerging Role of the CISO	Case 6 due
13	May 8	IT Risk Assessment Project Presentations		
14	May 15	IT Risk Assessment Project Presentations		Project Reports due

W&M = Michael W. Whitman and Herbert J. Mattord. *Principles of Information Security, Fifth Edition*. Cengage Learning, 2015 (selected material from this book will be posted on Canvas).

NIST = NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems. Available for download at http://csrc.nist.gov/publications/nistpubs/