Course Syllabus
MIS 6330

Naveen Jindal School of Management
The University of Texas at Dallas

Course Information

Course

Course Number Section	MIS6330.501.18S
Course Title	Information Technology Security
Term and Dates	Spring 2018

Professor Contact Information

Professor	Shaibal Chakrabarty
Office Phone	(214) 708-6163
Email Address	shaibalc@utdallas.edu
Office Location	Adjunct Offices
Office Hours	TBD
Other Information	The quickest and easiest way to contact me is through SMS or WhatsApp. We may set up a time to discuss your questions or discuss in class for benefit of all students.

Course Pre-requisite

MIS 6304 or MIS 6350

Course Description

The need for organizations to protect critical information assets continues to increase. Today, more than ever, organizations require professionals who understand technical issues and who are also capable of devising security strategies. Contrary to the common view, information security is mainly a managerial problem. Only through effective management of security, can security polices be defined and technical solutions be selected. The purpose of this course is to prepare business decision makers who recognize the threats and vulnerabilities present in existing systems and who know how to design and develop secure systems. This course (i) uses lectures to cover the different elements of information security, (ii) utilizes business cases and academic research studies to discuss information security issues faced by today's

businesses, (iii) demonstrates some popular security software using hands-on projects (iv) keeps in touch with the security market and practices through webcasts and video presentations (v) presents strategies and tools to develop an information security program within the organization.

Student Learning Objectives/Outcomes

1. Understand the challenges of securing information assets in a networked environment
2. Know the role and importance of each control layer in a defense-in-depth security architecture
3. Be able to conduct a security risk analysis to identify threats and vulnerabilities, and design an information security program to manage security risks
4. Recognize the basic categories of countermeasures to prevent, detect, and respond to security breaches

Required Textbooks and Materials

Required Texts

There is no required textbook for this course, but we will draw heavily from the two suggested texts.

Case Studies

1. Economics of Information Technology Security Management
2. The Sony Pictures Hack
3. The Mirae Botnet Attack
4. Digital Certificates and Signatures

Suggested Course Materials

Suggested Readings/Texts

1. Corporate Computer Security (4th edition) by Randy J. Boyle and Raymond R. Panko, Pearson, 2015, ISBN-10: 0133545199 ISBN-13: 9780133545197 (Note: You can also use the 3rd edition of this textbook.).

2. Computer Security: Principles and Practice (4th Edition) by William Stallings, Lawrie Brown, Pearson, ISBN-10: 0134794109, ISBN-13: 9780134794105

Suggested textbook can be ordered through the UTD Bookstore or Off-Campus Books. We will primarily use textbook #1 as a guide.

Suggested *Webcasts and Videos*

1. Big Brother Big Business: Surveillance vs. Privacy
2. Managing Updates Using Microsoft WSUS
3. Cyber War and Cyber Conflict

You are not going to be responsible from the contents of Webcasts and Videos in the tests.

You are encouraged to watch them in the week specified in the academic calendar (see the activity column) as they complement the material covered in that week's lecture.

Course Policies

Make-up tests, Extra Credit, and Late Work
The case assignments are due by the date given on the syllabus, and late assignments will not be accepted. There are no make-up tests or extra credit opportunities. If you know of a conflict in advance that will prevent you from
(i) taking a test within its scheduled time window, or
(ii) submitting your case assignment,
please inform me so we can try to work something out.

Class Participation
Students are required to participate, collaborate and contribute in class. There will be a grade assigned to class participation and collaboration.

Classroom Citizenship
Please use proper etiquette when interacting with class members and the professor.

Case Assignments

You will be assigned four case studies to analyze during the semester. You will answer some questions to complete each case assignment. The questions for case assignments will be available on eLearning. Each student is required to turn in a 3-page document containing answers to the posted case questions. Note that this is an individual assignment.

Before answering the questions, read the case carefully and take some notes of its key points (issues raised in the case, different approaches mentioned along with supporting arguments for each). Finally, read the questions posted on eLearning and answer them based on your understanding of the case. Some of the case questions will be open-ended questions. I will evaluate your answers based on their relevance to the question asked and your ability to integrate supporting arguments to defend your response. Case assignments will be worth 5% of the total points each and will count for 20% of your grade.

You can access assignments by clicking the Assignments link on the course menu. There is no time limit for case assignments (until the deadline). Although I will make the questions available at the beginning of the semester, I encourage you to work on an assignment only after listening to the lecture of the week in which the assignment is due. The due date for each assignment is indicated on the academic calendar section of this syllabus.

Assignment submission instructions

You will submit your assignments in a SINGLE PDF file format with a simple file name <FirstNameLastName>_<Exam/CaseStudy>_<number> by using the Assignments tool on the course site. Please see the Assignments link on the course menu or see the icon on the designated page. You can click each assignment name link and follow the on-screen instructions to upload and submit your file(s). Please refer to the Help menu for more information on using this tool. **Please note**: each assignment link will be deactivated after the assignment due time. After your submission is graded, you may click each assignment's "Graded" tab to check the results.

Grading Rubric for Case Assignments

Case questions are mostly open-ended questions. Hence, there is no one specific answer that we are looking for. Yet, we use some criteria to assess the quality of your answers.

Your case assignments will be graded based on the following criteria:

- Clear examples and at least two good points for each question - (4/4)
- Some examples and at least one good point for each question - (3/4)
- Extremely brief responses or an incorrect response for a question - (2/4)
- Incorrect responses for two or more questions - (1/4)
- No correct response or not submitting the assignment - (0/4)

Participation

You are expected to participate regularly in online discussions. A great deal of learning takes place when you share your experiences with others. Keep in mind that class participation is an important part of this course because it promotes learning through the dissemination of a variety of perspectives on a subject. Each week we will discuss security news of the week, and you will be asked to make a short presentation on a security topic of your choice. In addition grades may be assigned for some hands-on exercises on which questions will be asked. Participation is worth 10% of your grade.

The rules for participation in the discussion are as follows:

1) Participation points will be given for postings to online discussions. Each week there will be a discussion topic active under the title "Professor's Weekly Discussions - Week X". There will be a total of 14 topics discussed throughout the semester.

2) When a question is posted to professor's weekly discussion board, you can answer the question directly, or respond to the answers given by other students to mimic an in-class discussion. Look at this as a conversation with one another rather than trying to impress me with the "right" answer.

3) I am grading on quality of responses, not quantity. So, posts such as "I agree" or "sounds good to me" do not count towards participation (although you can certainly use these to advance the conversation. In order to count as participation your post has to be well thought out and pertain to the topic for the week. You should reference some of the concepts we are currently examining in class, not just offer vague assessments such as "there was a problem motivation". You can also refer back to previous weeks' material if relevant. Integration of concepts is the key since none of the issues operates completely independent of one another.

4) Keep discussion on topic and factual in nature. No flaming allowed. Opinions are fine as long as they are supported by facts. For example, stating that you think that a specific course of action is correct because of x, y, z is acceptable. Stating that the previous poster is an idiot is not.

5) Grammar and spelling are not graded in the discussion section, so don't feel that you have to spend hours editing your response. However, please use full words, not acronyms and abbreviations – not everyone is familiar with the text message language.

6) Limit your response to 250 words – any more than that and readers lose the point (and interest).

7) Each value-added comment posted to a discussion is worth 1 point, In order to receive full participation points you must post value-added comments 14 times during the semester. There is no minimum for a given week. However, to avoid some students from submitting their discussion posts in the last minute (i.e., at the end of the semester), each student will get at most two points for postings per week (even if a student posts 10 comments).

Hands-on Projects

Each week there will be an optional hands-on project. The objective of these projects is to give you an opportunity to interact with contemporary security solutions, ranging from scanning and analysis tools to encryption software. These tools are heavily used by security administrators, and you will get firsthand experience on using these popular security software tools. You will just follow step-by-step instructions to complete these projects. The hands-on projects are available in the suggested textbook. The hands-on projects are *not* graded.

Project 1: Nmap (Port Scanner) P. 51
Project 2: AxCrypt (Encryption Tool) P.179
Project 3: Cryptoanalysis P. 180
Project 4: inSSIDer (Diplaying Wireless Networks) P. 232
Project 5: Onion Routing (Providing anonymity) P. 233
Project 6: Wireshark (Packet Sniffer) p.359, 615, 616
Project 7: Windows Advanced Firewall (Blocking ICMP traffic) P.360
Project 8: File Verifier++ (File Integrity Checker) P.416
Project 9: TrueEncrypt (Creating Virtual Encrypted Disk) P. 521
Project 10: Eraser (Permanently Erasing Deleted Files) P.521
Project 11: HoneyBOT (Seeing the Probes and Scans) P.574
Project 12: Recuva (Recovering Deleted Files) P. 575

Tests

There will be two tests (open book and open notes) during the semester. Each is worth 20% of your grade. The first test will assess your knowledge on the subjects covered in the first six units (i.e., unit 1 through unit 6). The second test will include the rest of the units (i.e., unit 7 through unit 12).

Term Project/Research Paper

Your final project will be a paper that can be submitted to a reputed MIS Journal or conference. Your goal should target a submission for the AMCIS or ICIS (http://aisnet.org/page/Conferences) ; the Journal of the Association of Management Information Systems (http://aisel.aisnet.org/jais/). This paper and its research will comprise 30% of your total grade. This is a group project. You will form your team, pick a relevant topic, do your research, and provide updates and partial submissions approximately every 4 weeks, culminating in the final paper. The submission format and length will be identical to a journal or conference submission. Teams will be no more than 3 persons. On Week 12, each team will make a 15 min presentation of your paper. Only a single submission is required per team.

Top

Student Assessments

Grading Information

Weights

Test 1	20	20%
Test 2	20	20%
Case Assignments	20	20%
Participation	10	10%
Term Paper	30	30%
Total	100	100%

Grading criteria

Scaled Score	Letter Equivalent
92-100 %	A
88-92 %	A-
84-88 %	B+
80-84 %	B
76-80 %	B-
72-76 %	C+
68- 72 %	C
Less than 68 %	F

Accessing Grades

Students can check their grades by clicking “My Grades” under Course Tools after the grade for each assessment task is released.

Top

Technical Requirements

In addition to a confident level of computer and Internet literacy, certain minimum technical requirements must be met to enable a successful learning experience. Please review the important technical requirements on the Getting Started with eLearning webpage.

Top

Communications

Interaction with Instructor: I will communicate with students mainly using SMS, WhatsApp and Email tools. I will reply to student emails within 48-72 hours. If a matter is deemed urgent, instant messaging works best.

Discussion boards will provide broadcast communications to the class.

Top

Student Resources

The following university resources are available to students:

McDermott Library: Distance Learners (UTD students who live outside the boundaries of Collin**,** Dallas**,** Denton**,** Rockwall**,** or Tarrant counties) will need a UTD-ID number to access all of the library's electronic resources (reserves, journal articles, ebooks, interlibrary loan) from off campus. For UTD students living within those counties who are taking online courses, a Comet Card is required to check out materials at the McDermott Library. For more information on library resources go to http://www.utdallas.edu/library/distlearn/disted.htm.

Top

Academic Calendar

WEEK/ DATES	MODULE	UNIT(LECTURE)	ASSESSMENT / ACTIVITY	DUE DATE
1 Jan 9 Jan 15	Module 1: Foundations of Information Security Management	Unit 1: Introduction to Information Security	Self Quiz Course Orientation: Syllabus Hands-on Project 1	
2 Jan 16 Jan 22	Module 1: Foundations of Information Security Management	Unit 2: Common Forms of Attacks	Self Quiz Video Presentation: Cyber War and Cyber Conflict Hands-on Project 2	
3 Jan 23 Jan 29	Module 1: Foundations of Information Security Management	Unit 3: Information Security Programs	Self Quiz Hands-on Project 3	Case Assignment 1: Economics of IT Security Management (Jan 29, 11:59 pm)
4 Jan 30 Feb 5	Module 1: Foundations of Information Security Management	Unit 4: Information Privacy, Compliance, and Cyber Laws	Self Quiz Video Presentation: Big Brother Big Business: Surveillance vs. Privacy Hands-on Project 4	
5 Feb 6 Feb 12	Module 1: Foundations of Information Security Management	Unit 5: Access Controls	Self Quiz Hands-on Project 5	Case Assignment 2: Microsoft Security Response Center (A) (Feb 12, 11:59 pm)

6 Feb 13 Feb 19	Module 2: Network and Host Security	Unit 6: Network Fundamentals	Self Quiz Hands-on Project 6	
7 Feb 20 Feb 26	**TEST 1** **(Available between Feb 23, 12:01 am and Feb 26, 11:59 pm)**			
8 Feb 27 March 5	Module 2: Network and Host Security	Unit 7: Network Security	Self Quiz Hands-on Project 7	Case Assignment 3: IPremier Company DOS Attack (A) (March 5, 11:59 pm)
9 March 6 March 12	Module 2: Network and Host Security	Unit 8: Host Security	Self Quiz Webcast: Managing Updates Using Microsoft WSUS Hands-on Project 8	
10 March 13 March 19	**SPRING BREAK**			
11 March 20 March 26	Module 2: Network and Host Security	Unit 9: Detective Controls	Self Quiz Hands-on Project 9	
12 March 27 April 2	Module 3: Data and Communications Security	Unit 10: Principles of Communications Security	Self Quiz Hands-on Project 10	

13 April 3 April 9	Module 3: Data and Communications Security	Unit 11: Communications Security Technologies	Self Quiz Hands-on Project 11	Case Assignment 4: Digital Certificates and Signatures (April 9, 11:59 pm)
14 April 10 April 16	Module 3: Data and Communications Security	Unit 12: Cryptographic Systems	Self Quiz Hands-on Project 12	
15 April 17 April 23	**TEST 2** **(Available between April 20, 12:01 am and April 23, 11:59 pm)**			

Top

Scholastic Honesty

The University has policies and discipline procedures regarding scholastic dishonesty. Detailed information is available on the UTD Judicial Affairs web page. All students are expected to maintain a high level of responsibility with respect to academic honesty. Students who violate University rules on scholastic dishonesty are subject to disciplinary penalties, including the possibility of failure in the course and/or dismissal from the University. Since such dishonesty harms the individual, all students and the integrity of the University, policies on scholastic dishonesty will be strictly enforced.

Course Evaluation

As required by UTD academic regulations, every student must complete an evaluation for each enrolled course at the end of the semester. An online instructional assessment form will be made available for your confidential use. Please look for the course evaluation link on the course Home Page towards the end of the course.

University Policies

The information contained in the following link constitutes the University's policies and procedures segment of the course syllabus.

Please go to http://go.utdallas.edu/syllabus-policies for these policies.

These descriptions and timelines are subject to change at the discretion of the Professor.

Top