MIS 4360-501
Network and Information Security
Spring 2013

Professor: **Huseyin Cavusoglu, Ph.D.**
Phone: (972) 883-5939
Office: SOM 3.418
Email: eLearning Email
TA: Zhen Sun, zxs098020@utdallas.edu

Class Hours: Tuesday 7:00 - 9:45 p.m. JSOM 2.722
My Office Hours: Tuesday 6:00 - 7:00 p.m. or by appointment.

Case Book (Required)

1. MIS 4360 Course pack (Available at UTD Bookstore)

Suggested Textbook (Optional)

1. Corporate Computer and Network Security (Second Edition) by Raymond R. Panko, Prentice Hall, 2010, ISBN-10: 0131854755, ISBN-13: 978-0131854758

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 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, (iv) keeps in touch with security market and practices through webcasts, video presentations, guest speakers (v) presents strategies and tools to develop an information security program within the organization.

Grading: eLearning will be used to help with the course and grading

Exam1 (35 %)
Exam 2 (35 %)
Case Assignments (10 %)
Class Contribution (10 %)
Research Project (10 %) - (5% presentation and 5% final report)

I will ensure that grading is fair and consistent for all students. If you are not satisfied with your grade, please meet me to discuss the issue. Please note that there will be NO make-up exam or additional assignment for extra grade.

I will assign a letter grade based on the semester average of each student. I will use the following criteria:

Semester Average	**Letter Grade**
96-100	A+
92-96	A
88-92	A-
84-88	B+
80-84	B
76-80	B-
72-76	C+
68-72	C
64-68	C-
60-64	D+
56-60	D
52-56	D-
0-52	F

Lectures

In the first half of each class, we will have a regular lecture that will cover material from the textbook and other sources. The purpose of these lectures is to make you familiar with the basic security concepts and methods. In the first module (lectures 1-5), we are going to study the *foundations of information security management*. The second module (lectures 6-9) is going to emphasize *network and host security*. Finally, the third module (lectures 10-12) is going to discuss *data and communications security*. The PowerPoint slides will be made available on eLearning as lecture notes before the class.

Cases, Webcast, Software Demonstrations, Video Presentations, and Guest Speakers

In the second half of each class, we will augment our lectures using (i) case studies, (ii) software demonstrations, (iii) guest speakers, (iv) video presentations, and (v) webcasts. This part will build on the material covered in lectures and will improve the understanding of issues surrounding information security. The case studies include three cases from the Harvard Business School Publishing (HBSP) and one of my academic studies. For Harvard cases, I have created a course pack. You can purchase it from the UTD bookstore. It is very important that everybody gets his/her own copy of the course pack. The amount you pay also covers the cost of supplemental material (copyrighted) that I will distribute during case discussions. All other materials for non-lecture parts will be posted on the eLearning course site.

Case Questions, Discussions, and Assignments

I will prepare some questions for each case that will guide our discussion of the case studies. I will make these questions available on eLearning prior to class. Each student is expected to prepare for discussion of the relevant case before coming to class. In addition, *each student*

is required to turn in a 2-page document containing answers to the posted case questions before the class for the case discussion. Note that this is an individual assignment.

First, read the case carefully. Take some notes of key points (the issue raised in the case, different approaches mentioned along with supporting arguments for each of them). Finally, read the questions posted on eLearning and try to come up with some answers. Identify the key take-away from the case. During case discussions, I expect all of you to participate. I also encourage you to share your experiences whenever you deem them relevant to the case.

Class Contribution

Your class contribution will be determined by (i) the quality and appropriateness of comments (ii) the relevance and intelligence of questions asked, (iii) answers to the questions asked by the instructor, and (iv) expression of interesting opinions, in both lecture and non-lecture parts. In addition, you will get credit for contributions to online discussions. I will start a new online discussion on eLearning each week. Keep in mind that class contribution is an important part of this course because it promotes learning through dissemination of a variety of perspectives on a subject. I will also cold call on students who have not participated in class discussions for a while.

Group Project

As part of the requirements for this course, students will work in groups on a security project. Each project topic captures the issues that cause heated discussion among security professionals today. The goal of these projects is to give you a chance to conduct rigorous research on hot security issues. You are expected to examine various aspects of the topic from different perspectives. You will present your findings to the class at the end of the semester. Each group will choose one of the topics provided below.

- Return on Security Investment (ROSI)
- Cyber Insurance
- Security Information and Event Management (SIEM)
- Cloud Computing, Virtualization, and Security
- Digital Forensics
- Security Metrics
- SOX and Security
- Security Auditing
- PCI Compliance
- Security Outsourcing (MSSPs)

The size of the class will determine the group size. You will be able to sign up for group projects on eLearning once I determine the appropriate group size. There are two deliverables for this project:

i) Presentation: During the presentation you will share your findings with other students, explaining the most important aspects of the issue and highlighting the pros and cons of different solution methodologies. After the presentation, there will be a question and answer session and an open discussion.
ii) Final Report: Each group will write a paper covering the issues discussed in the presentation. This paper should be between 8 and 10 pages, one and a half spaced, 12 point font. You should highlight the interesting aspects of the problem in your paper. Also you should objectively cover proposed solution methodologies with their strengths

and weaknesses. Use a third-person narration (avoid using we and/or I). Do not forget to cite the sources (references). It is due by the end of the class on April 30.

The group projects will be evaluated according to following criteria:

1) technical completeness (the extent to which technical issues are addressed)
2) managerial relevance (the extent to which business considerations are included)
3) quality of the paper and presentation (prioritization and categorization of ideas, clarity of language used, adequate answers to questions raised)

Security News Sources

Each student is urged to subscribe to *Information Security Magazine*. This magazine covers stories about recent developments in security and security community. Its perspective is broad, focusing on both technical and managerial issues. You can get this valuable magazine free by filling out a form at
http://searchsecurity.techtarget.com/regPage1/1,296503,sid14,00.html

You can also become a member of *SearchSecurity.com* to receive tailored e-mails on the topics that interest you most, with the latest news, technical papers, site surveys and IT announcements that match your unique profile. You can subscribe to this service at http://searchsecurity.techtarget.com/regPage1/1,296503,sid14,00.html

Becoming an ISACA Student Member

ISACA (Information Systems Audit and Control Association) is a global organization for IT professionals focusing on information governance, security, and audit. As a student member, you will join a network of thousands of professionals working in industry, academia and government. It has 170 local chapters worldwide providing education, resource sharing, advocacy, professional networking. Benefits of student membership include electronic subscription to the *Information Systems Control Journal*, free downloads of publications such as COBIT® (Control Objectives for Information and related Technology), and discounts on ISACA certifications (CISA, CISM), events, and conferences. Just complete the application at www.isaca.org/student to become a student member.

Classroom Rules and Etiquette

Any act of classroom disruption that goes beyond the normal rights of students to question and discuss with the instructor the educational process relative to subject content will not be tolerated. Specifically:
You are not allowed to use your laptops, PDAs and other electronics during the class for checking email or surfing the Internet. Your cooperation with this rule is greatly appreciated. Cell phones and pagers should either be turned off or placed in a quiet state (vibrate) during class. If your cell phone or pager cannot be placed in a quiet state, please turn it off. Students will not be excused during an exam to answer cell phone calls.

Student Conduct and Discipline

The University of Texas System and The University of Texas at Dallas have rules and regulations for the orderly and efficient conduct of their business. It is the responsibility of each student and each student organization to be knowledgeable about the rules and regulations which govern student conduct and activities. General information on student

conduct and discipline is contained in the UTD publication, *A to Z Guide*, which is provided to all registered students each academic year.

The University of Texas at Dallas administers student discipline within the procedures of recognized and established due process. Procedures are defined and described in the *Rules and Regulations, Board of Regents, The University of Texas System, Part 1, Chapter VI, Section 3*, and in Title V, Rules on Student Services and Activities of the university's *Handbook of Operating Procedures*. Copies of these rules and regulations are available to students in the Office of the Dean of Students, where staff members are available to assist students in interpreting the rules and regulations (SU 1.602, 972/883-6391).

A student at the university neither loses the rights nor escapes the responsibilities of citizenship. He or she is expected to obey federal, state, and local laws as well as the Regents' Rules, university regulations, and administrative rules. Students are subject to discipline for violating the standards of conduct whether such conduct takes place on or off campus, or whether civil or criminal penalties are also imposed for such conduct.

Academic Integrity

The faculty expects from its students a high level of responsibility and academic honesty. Because the value of an academic degree depends upon the absolute integrity of the work done by the student for that degree, it is imperative that a student demonstrates a high standard of individual honor in his or her scholastic work.

Scholastic dishonesty includes, but is not limited to, statements, acts or omissions related to applications for enrollment or the award of a degree, and/or the submission as one's own work or material that is not one's own. As a general rule, scholastic dishonesty involves one of the following acts: cheating, plagiarism, collusion and/or falsifying academic records. Students suspected of academic dishonesty are subject to disciplinary proceedings.

Plagiarism, especially from the web, from portions of papers for other classes, and from any other source is unacceptable and will be dealt with under the university's policy on plagiarism (see general catalog for details). This course will use the resources of turnitin.com, which searches the web for possible plagiarism and is over 90% effective.

Withdrawal from Class

The administration of this institution has set deadlines for withdrawal of any college-level courses. These dates and times are published in that semester's course catalog. Administration procedures must be followed. It is the student's responsibility to handle withdrawal requirements from any class. In other words, I cannot drop or withdraw any student. You must do the proper paperwork to ensure that you will not receive a final grade of "F" in a course if you choose not to attend the class once you are enrolled.

Student Grievance Procedures

Procedures for student grievances are found in Title V, Rules on Student Services and Activities, of the university's *Handbook of Operating Procedures*.

In attempting to resolve any student grievance regarding grades, evaluations, or other fulfillments of academic responsibility, it is the obligation of the student first to make a serious effort to resolve the matter with the instructor, supervisor, administrator, or committee with whom the grievance originates (hereafter called "the respondent"). Individual faculty members retain primary responsibility for assigning grades and evaluations. If the matter cannot be resolved at that level, the grievance must be submitted in writing to the respondent with a copy of the respondent's School Dean. If the matter is not

resolved by the written response provided by the respondent, the student may submit a written appeal to the School Dean. If the grievance is not resolved by the School Dean's decision, the student may make a written appeal to the Dean of Graduate or Undergraduate Education, and the deal will appoint and convene an Academic Appeals Panel. The decision of the Academic Appeals Panel is final. The results of the academic appeals process will be distributed to all involved parties.

Copies of these rules and regulations are available to students in the Office of the Dean of Students, where staff members are available to assist students in interpreting the rules and regulations.

Incomplete Grades

As per university policy, incomplete grades will be granted only for work unavoidably missed at the semester's end and only if 70% of the course work has been completed. An incomplete grade must be resolved within eight (8) weeks from the first day of the subsequent long semester. If the required work to complete the course and to remove the incomplete grade is not submitted by the specified deadline, the incomplete grade is changed automatically to a grade of **F**.

Disability Services

The goal of Disability Services is to provide students with disabilities educational opportunities equal to those of their non-disabled peers. Disability Services is located in room 1.610 in the Student Union. Office hours are Monday and Thursday, 8:30 a.m. to 6:30 p.m.; Tuesday and Wednesday, 8:30 a.m. to 7:30 p.m.; and Friday, 8:30 a.m. to 5:30 p.m.

The contact information for the Office of Disability Services is:
The University of Texas at Dallas, SU 22
PO Box 830688
Richardson, Texas 75083-0688
(972) 883-2098 (voice or TTY)

Essentially, the law requires that colleges and universities make those reasonable adjustments necessary to eliminate discrimination on the basis of disability. For example, it may be necessary to remove classroom prohibitions against tape recorders or animals (in the case of dog guides) for students who are blind. Occasionally an assignment requirement may be substituted (for example, a research paper versus an oral presentation for a student who is hearing impaired). Classes enrolled students with mobility impairments may have to be rescheduled in accessible facilities. The college or university may need to provide special services such as registration, note-taking, or mobility assistance.

It is the student's responsibility to notify his or her professors of the need for such an accommodation. Disability Services provides students with letters to present to faculty members to verify that the student has a disability and needs accommodations. Individuals requiring special accommodation should contact the professor after class or during office hours.

Religious Holy Days

The University of Texas at Dallas will excuse a student from class or other required activities for the travel to and observance of a religious holy day for a religion whose places of worship are exempt from property tax under Section 11.20, Tax Code, Texas Code Annotated.

The student is encouraged to notify the instructor or activity sponsor as soon as possible regarding the absence, preferably in advance of the assignment. The student, so excused, will be allowed to take the exam or complete the assignment within a reasonable time after the absence: a period equal to the length of the absence, up to a maximum of one week. A student who notifies the instructor and completes any missed exam or assignment may not be penalized for the absence. A student who fails to complete the exam or assignment within the prescribed period may receive a failing grade for that exam or assignment.

If a student or an instructor disagrees about the nature of the absence [i.e., for the purpose of observing a religious holy day] or if there is similar disagreement about whether the student has been given a reasonable time to complete any missed assignments or examinations, either the student or the instructor may request a ruling from the chief executive officer of the institution, or his or her designee. The chief executive officer or designee must take into account the legislative intent of TEC 51.911(b), and the student and instructor will abide by the decision of the chief executive officer or designee.

Tentative Schedule

Date	Lecture	Lecture Material	Non-Lecture
January 15	**1. Introduction to Information Security** History of Security, Principles of Information Security, Security Process, Defense-in-Depth: Layered Security	Lecture Notes	
January 22	**2. Common Forms of Attacks** Social Engineering, Denial-of-Service, IP Spoofing, Buffer Overflow, Malware Attacks, Spyware, Phishing, and Botnets	Chapter 1 Lecture Notes	**Webcast:** How Hackers Hack
January 29	**3. Information Security Programs** Security Policies, Procedures and Guidelines; Security Education, Training and Awareness; Risk Management; Contingency Planning	Chapter 2 Chapter 9 Lecture Notes	**Case:** Economics of IT Security (on eLearning)
February 5	**4. Information Privacy, Compliance, and Cyber Laws** Privacy Concerns, Customer Expectations, Corporate Responses, Monitoring; HIPPA, GLBA, SB 1386, PCI DSS; Laws governing Computer Crime; Cyber War/Terrorism	Lecture Notes	**Video:** Big Brother Big Business: Surveillance vs. Privacy
February 12	**5. Access Controls** Authentication: Password, Biometrics, Token, CHAP, Kerberos, Multi-factor; Authorization: ACL; Wireless Authentication (WEP, 802.1x)	Chapter 5 Lecture Notes	**Guest Speaker:** Rick Holland *Forrester Research* Senior Analyst Security & Risk Management
February 19	**6. Network Fundamentals** Review of TCP/IP, OSI Architecture, Connectionless and Connection-Oriented Services, IP addressing, IP Address Masking, IP Packets, Ports, ICMP	Module A Lecture Notes	**Case (HBSP)**: IPremier Company DOS (A)

February 26	**7. Network Security** Firewalls: Packet-Filtering, State-Inspection, Application-Level; NAT; Enterprise Firewall Architecture, Desktop Firewall Architecture, Firewall Products	Chapter 6 Lecture Notes	**Review Session for Exam 1**
March 5	**EXAM 1 (Lecture 1 through Lecture 6)**		
March 12	**Spring Break – NO CLASS**		
March 19	**8. Host Security** Host Hardening: Configuration, Fixing Vulnerabilities, Managing Users, Groups, and Permissions, Logging; Testing for Vulnerabilities; Hardening Clients: NAC	Chapter 7 Lecture Notes	**Webcast**: Microsoft Solutions for Patch Management
March 26	**9. Detective Control** Intrusion Detection Systems: Network-Based vs. Host-Based, Signature vs. Anomaly Detection, Active vs. Passive Response; SNORT; Base-Rate Fallacy, Configuration of IDS, Value of IDS; IPS	Chapter 10 Lecture Notes	**Case (HBSP)**: Microsoft Security Response Center (A)
April 2	**10. Principles of Communications Security** Secure Communication Services; Encryption: Public Key vs. Symmetric Key; Encryption Methods: DES. 3DES, AES, RSA; Diffie-Hellman Key Agreement	Chapter 3 Lecture Notes	**Webcast:** Decoding Nazi Secrets
April 9	**11. Communications Security Technologies** Hybrid Encryption; Hashing; Digital Signatures, Digital Certificates, Certificate Authorities, PKI; Steganography	Chapter 3 Lecture Notes	**Case (HBSP):** Digital Certificates and Signatures
April 16	**12. Cryptographic Systems** Cryptographic System Stages, Major Cryptographic Systems: SSL/TLS, IPSec, Kerberos; VPNs, Securing E-Mail: S/MIME, PGP	Chapter 3 Chapter 4 Chapter 8 Lecture Notes	**Software Demonstration:** Encryption Tools, Scanning and Analysis Tools
April 23	**Group Presentations**		
April 30	**EXAM 2 (Lecture 7 through Lecture 12)**		