BCIS 5630
Information Technology Security

COURSE INFORMATION

Instructor: Dan J. Kim
Email: Dan.Kim@unt.edu (preferred contact method)
Phone: (940) 369 - 8942
Office: 312D Business Leadership Building (BLB)
Class Hours: Monday 6:30 – 9:20 PM
Class Room: BLB 075
Office Hours: Monday and Wednesday 11:00 - 12:00 PM (or by appointment)
Course Web Site: ecampus.unt.edu and drobox.com

Required Textbook and Readings:

- Joseph Migga Kizza, *Ethical and Social Issues in the Information Age*, Fifth Edition, 2013, ISBN ISBN 978-1-4471-4989-7

- Published journal articles and other materials be retrieved from the course website

COURSE OVERVIEW

This is a graduate-level interdisciplinary course on Information Security which covers the various technical, managerial, social, and socio-technical aspects of information security. Students will be exposed to the spectrum of security management activities including security investigation and analysis, risk management, implementation and maintenance of information assurance, ethical, legal and professional aspect of information security and assurance.

Students will be also exposed to research topics related to the information security and assurance discipline. It is expected that students develop in-depth understanding and knowledge on information security and information assurance through lectures, discussions, and presentations of topics and issues covered in class. It is also expected that the student will start the research apprenticeship as a part of course project and produce a research paper worthy of submission to a conference at least.

LEARNING OUTCOMES

Upon successful completion of this course, students will be able to:

- Explain why information security management is so important today for business and management
- Define risk management and discuss the stages in the risk management process.
- Develop the information security planning process.
- Develop the various types of contingency planning.
- Design a security awareness and education program.
- Identify and evaluate potential researchable topics on information security
- Conduct literature review on a suitable research topic
- Understand the writing processes of a research paper
- Develop research paper writing skills for a referred conference/journal publication

TENTATIVE COURSE SCHEDULE AND READINGS

The following pages provide basic information about the class schedule and each of the items above. Additional information will be provided in class. The scheduled dates for deliverables are subject to change, but all changes will be discussed in class. All students must turn in required work at the scheduled times except for emergencies.

TENTATIVE COURSE SCHEDULE

	Date	Topics	Assignment and Due
W1	Jan. 26	Course introduction What is Research?	
W2	Feb. 2	C1: History of Computing C2: Morality and the Law C3: Ethics and Ethical Analysis C4: Ethics and the Professions	Starting individual meeting with the instructor to find a research topic
W3	Feb. 9	C5: Anonymity, Security, Privacy, and Civil Liberties C6: Intellectual Property Rights and Computer Technology C7: Social Context of Computing	
W4	Feb. 16	C8: Software Issues: Risks and Liabilities C9: Computer Crimes C10: New Frontiers: Artificial Intelligence	
W5	Feb. 23	C11: New Frontiers: Virtualization and Virtual Reality C12: New Frontiers: Cyberspace C13: Ethical, Privacy, and Security Issues in the Online Social Network Ecosystem	P1: Research topic analysis and proposal due
W6	Mar. 2	C14: Mobile Systems and Their Intractable Social, Ethical and Security Issues C15: Computer Crime Investigations and Ethics C16: Biometrics Technologies and Ethics	
W7	Mar. 9	**Midterm**	
W8	Mar. 16	Spring Break (No Class)	
W9	Mar. 23	Selected Topic 1: Current Issues on Information Security	
W10	Mar. 30	Selected Topic 2: Security Policy Compliance	P2:Literature review and conceptual model
W11	Apr. 6	Selected Topic 3: Security Threat and Coping Malicious Artifacts	
W12	Apr. 13	Selected Topic 4: Security Risk Management	P3: Theory building: hypothesis and methodology
W13	Apr. 20	Selected Topic 5: Information Privacy Issues in the Internet	
W14	Apr. 27	Selected Topic 6: Organizational Privacy Practices	
W15	May. 4	Research Paper Presentation	P4: Final paper due
Note: 1) The schedule and course outline are subject to change, depending on class pace and needs. The instructor reserves the rights to make any changes needed. 2) According to University Regulations, a grade of Incomplete can only be given if the student is currently passing the course. This is only given when circumstances prevent you from completing the semester.			

GRADING

The final letter grades for this course will be determined based on following:

1. Class participation (30%)
2. Mid-term Exam (30%)
3. Research paper project (40%)

1. Class Participation

Class attendance is mandatory. Each student is expected to actively participate in every class. The final grade will be determined on the basis of the quality of student's preparation and participation. It is core of this course to read and critical analyze the reading and then actively participate in the discussion of the issues in class. **Each student or team will be responsible for presentation and leading the discussion over the course of the semester.**

a. Textbook chapter presentation and discussion

A group of students will be assigned primary responsibility for each chapter from the textbook. As a presentation group of each chapter, the group has to: 1) prepare a 20-25 minute ppt presentation slides of the assigned chapter, 2) upload the ppt file to the course website a day BEFORE the class, 3) present the presentation, and 4) lead the subsequent class discussion about 10 minutes.

b. Assigned article write-up, presentation, and discussion

A group of students will be assigned for each research article. The group needs to: 1) prepare a single spaced 1-2 page write-up and a 15-20 minute opening presentation of the assigned article, 2) upload the write-up and ppt slides to the course website BEFORE the class, 3) distribute a copy of the write-up at class, 4) present a summary of the key points using ppt slides, and 5) lead the subsequent class discussion on the research article. A sample template of write-up will be given.

After presenting a summary of the key points, the subsequent class discussion is the key element of class participation, which should have at least three components.

a) Assessment of key contributions in terms of theory and practice
b) Discussion of the strengths and weakens, and
c) Presentation of future (possible your) work that can build on the study

2. Mid-term Exam

There will be one mid-term examination. The content will come from the textbook and other material discussed in class sessions. There will be no make-up examination. It is the student's responsibility to arrange for an excused absence before the exam. A grade of zero will be assigned for the exam missed without an excused absence.

3. Research Paper Project

Each student will be required to complete either *a complete empirical, technical, or comprehensive review research paper* in the areas related to cyber security.

For the empirical research paper project, four key elements should be in place. a) The paper should address a substantial issue in the area of study. b) You should have an empirical data in hand or possibly collaborate with other person who has an empirical data. c) It should have a strong theoretical perspective – it would be good idea to expand from or build on existing theory. d) It should explicitly address unique theatrical and practical contributions.

For the technical/practical paper project, following key elements should be in place. a) The paper should address a substantial technical/practical issue in the area of study. b) You should find or propose a technical solution of the issue. c) It should have a strong practical perspective. d) It should explicitly address unique theatrical and practical contributions.

For the theoretical/review project, I expect you produce a theory review paper that would be publishable as an MISQ Review piece. It should have the following four key elements. a) A research topic area where there is diverse research that can benefit from synthesis in order to clarify knowledge coalesced. b) It should promote research by surveying and synthesizing prior theoretical and empirical research - it could possibly involve meta-analysis. c) It should clearly discuss future research directions. d) Finally, it should act as a repository for the knowledge that has been accumulated on an important topic within the information security field and advance theory in that topic area.

This assignment especially aims to help you in developing and writing a research paper, your master thesis or Ph.D. dissertation proposal. Details concerning the content of each phase, due dates for submission and revisions are provided below. Note that to maintain satisfactory progress toward a timely completion of the paper, it is essential that you submit your best-effort drafts by the specified due dates.

a. First Phase: Topic Analysis and Proposal (2/23)

Describe the substantive issue under investigation and be specific as possible about:

- The related knowledge and other relevant background information
- Research paper purpose
- Research paper objective and research questions
- Potential contributions to knowledge and implications

b. Second Phase: Literature Review and Conceptual Model (3/30)

Set a conceptual testable model and frame it in the context of the literature:

- Describe overall rationale of your theory
- Specify available your model (either empirical or analytic model)
- Identify the main constructs for your model
- Identify the relationships between the constructs
- Conduct an extensive literature review
- Attach a drawing of the conceptual model

c. Third Phase: Theory Building: Hypothesis and Methodology (4/13)

Students should suggest research design:

- Describe how you intend to test the model
- Formulate a set of testable hypotheses concerning the relationships between the constructs
- Identify possible data sources and each of the hypothesized relationships
- Identify possible scales or other applicable instruments
- Attach a table that lists the constructs, their definitions, and their main references.

d. Fourth Phase: Final Paper and Presentation (5/4)

- The final paper should be about 14 pages in single space including references. You can use the ICIS submission guideline of complete research paper http://icis2015.aisnet.org/images/docs/ICIS_Original_Submission_Template.doc

USEFUL RESOURCES

- SaTC Cyber Café, Research Topic Breakout Sessions, National Science Foundation, http://www.satc-cybercafe.net, 2012
- Data for Cybersecurity Research: Process and "Wish List", National Science Foundation, https://www.gtisc.gatech.edu/nsf_workshop10, 2010
- Dear Colleague Letter requesting new collaborations between computer scientists and social scientists, http://www.nsf.gov/pubs/2013/nsf13037/nsf13037.jsp
- Proceedings of The Dewald Roode Information Security Workshop, http://ifip.byu.edu
- Reference book: Business Research Methods, by Cooper and Schindler, McGraw-Hill Irwin, 2002.
- Theories used in IS Research http://www.fsc.yorku.ca/york/istheory/wiki/index.php/Main_Page
- Theory Clusters http://www.tcw.utwente.nl/theorieenoverzicht/Theory%20clusters/
- Design Research in Information Systems http://desrist.org/design-research-in-information-systems/
- Qualitative Research in Information Systems http://www.qual.auckland.ac.nz/
- Quantitative, Positivist Research Methods in Information Systems: http://dstraub.cis.gsu.edu:88/quant/

ABOUT THE PROFESSOR

Dan J. Kim is Professor of Information Technology and Decision Sciences (ITDS) at University of North Texas. He earned his Ph.D. in MIS from SUNY at Buffalo. He also holds a MBA degree with management science concentration and MS degree in computer science. His research interests are in multidisciplinary areas such as information security (InfoSec) and privacy, information assurance, and trust in electronic commerce. Recently he has focused on InfoSec Self-Efficacy, Web Assurance Seal Services, Social Networking, and Trust in e-collaborations. His research work has been published or in forthcoming more than 120 papers in refereed journals, peer-reviewed book chapters, and conference proceedings including *Information Systems Research, Journal of Management Information Systems, Communications of ACM, Communications of AIS, Decision Support Systems, International Journal of Human-Computer Interaction, Journal of Organizational and End User Computing, IEEE Transactions on Professional Communication, Electronic Market, IEEE IT Professional, Journal of Global Information Management, and International Journal of Mobile Communications, ICIS, HICSS, AMCIS, INFORMS, and so on.* He has been awarded the National Science Foundation CyberCorps: SFS grant for multi-years, 2012 Emerald management Review Citations of Excellence Awards, 2010 Best Published Paper Award in ISR, an Emerald Literati Network 2009 - Outstanding Paper Award, the AMCIS 2005 Best Research Paper Award at AMCIS 2005 and the ICIS 2003 Best Paper-First Runner-up Award. He was ranked at 22nd worldwide in terms of research productivity from year 2008 to 2010 based on top three leading IS journals: ISR, MISQ and JMIS.

ACADEMIC INTEGRITY

The standards of academic integrity of the University of North Texas will be strictly enforced. Please refer to the undergraduate handbook for details. Students cannot use any assignments that have been part of earlier sections of the course. Cheating will not be tolerated. Students found cheating will receive a grade of F for the course and subject to further disciplinary action by University of North Texas.

Plagiarism is defined as presenting another person's work or ideas as one's own. You are expected to do your work on all assignments. Students who plagiarize will receive a Fail grade in the course.

Please refer to the links below for the course ground rules and academic honesty policy in details.
http://policy.unt.edu/sites/default/files/untpolicy/pdf/7-Student_Affairs-Academic_Integrity.pdf