ITM 640: Information Security Risk Assessment Syllabus

Sanjay Goel
School of Business
University at Albany, State University of New York

INSTRUCTOR INFORMATION

Name: Sanjay Goel
Email: goel@albany.edu
Phone: (518) 442-4925
Office Location: BA 310b, University at Albany
Office Hours: TBD

CLASS INFORMATION

Time: N/A
Location: Online
Dates: TBD
Credit(s): 3
Call #: TBD

RESOURCES

Course Website: The course website is located at the West Lafayette Open Campus Blackboard web system: http://www.itap.purdue.edu/tlt/blackboard/open.cfm
Click on "Log On" and sign in using the Username and Password assigned to you via email.

Readings: Reference readings will be posted at the end of each presentation. Available readings will be accessible via http://eres.ulib.albany.edu

You must click on "Electronic Reserves & Reserve Pages" and then type in "INF740" in the empty box. Click under the Course Number section (which is hyperlinked) you will be asked to input a password. The password to access this information will be provided via email and is case-sensitive. All of the readings is divided by Unit and contains readings in .pdf format or web links to readings.

Reference Books:
Secrets & Lies by Bruce Schneier
Hackers Beware by Eric Cole

COURSE OVERVIEW

This course provides students with an introduction to the field of information security risk assessment. Initially, the students will be introduced to basic definitions and nomenclature in the area of security assessment. Thereafter they will be taught different approaches for assessment of risk. The course will incorporate cases in risk analysis derived from actual state and law enforcement agencies or private firms. Students will learn how to use a risk analysis matrix for performing both quantitative and qualitative risk analysis. As a part of the course, students learn of the different threats that they need to incorporate in their risk analysis matrices.

Course Prerequisites
It is assumed that students will come in with varied backgrounds in information systems with some general background of computer security. It would be helpful if students have some knowledge of the following topics:

1. Computer Networks
2. Computer Architecture
3. Software Design
4. Statistical and Probabilistic Analysis
5. Basic Information Security

Course Format

This course is being offered as an online course through the help of CERIAS and Purdue University. However, the intent of the course is to provide students with an interactive learning environment through instructor audio, discussion groups, and interactive quizzes. The purpose of the course is to train students in the practice of risk analysis by elucidating the concepts through examples and case studies. Students are expected to use critical thinking skills as they go through the material rather than accepting facts at face value. Even though the course is spread over several weeks it is important that students stay on schedule so that they can participate with other students in discussions. The class should require approximately 120 hours of work including instruction video of lecture material, quizzes, discussion postings, final project, and readings.

Learning Objectives

At the end of the course, students should be able to:

1. Understand the basic nomenclature and definitions of risk analysis
2. Develop a work plan for executing a risk analysis in the organization
3. Understand the various threats to information assets in the organization
4. Identify and value assets
5. Determine exploitable vulnerabilities
6. Determine threats to an organizational system
7. Recommend controls to mitigate risk
8. Aggregate the data qualitatively and quantitatively to perform risk analysis

ASSESSMENT & GRADING

Academic Integrity Compliance: Students MUST comply with all University standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** If a student is discovered to NOT comply with academic integrity standards, the student will be reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive either a warning, be told to rewrite the plagiarized material, receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Examples of violations include: Giving or receiving unauthorized help before, during, or after an examination; Collaborating on projects, papers, or other academic exercises which is regarded as inappropriate by the instructor(s), Submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being (and has in the past been) submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (for example, the words, ideas, information, code, data, evidence, organizing principles, or style of presentation of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, the purchase of prepared research, papers, or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a

form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations.

If you ever have any questions about whether you could be violating academic integrity standards - ASK!

Grading Rubric

Quizzes/Exams (20%) – Please work individually on all quizzes/exams. Two exams will be offered after during the course. Please go to the Toolbar and click "Other Tools". Select "Assessments" and you will see the exams. This will be graded automatically via Blackboard.

Discussion Postings (30%) – Even though this is an online course, it is expected that students will be able to learn from each other and participate in a discussion. To promote this, you will be assigned discussion postings, which will be graded. Discussions will be able to be created and viewed by going to the "Discussions" link on the top right hand corner of the page. In addition to discussion postings, responses to other student posts are also required. Initial postings will generally be due on Wednesday and responses to other postings should be up by the Sunday of that week.

Project (50%) – The end of semester project involves the use of both qualitative and quantitative risk analysis methodologies described within the lecture and should be due after the end of the class on ***INSERT DATE*** through the Blackboard interface (taking into account the other course students are also taking). To do this, go to "Other Tools" on the Toolbar on the right-hand corner and click on "Assignments". Select "Risk Analysis Project". This should be done based on your own existing organizations (or another real organization). Make sure to scope the work appropriately.

First, collect the data on assets, threats, vulnerabilities, and controls. Use the spreadsheet provided to fill in the tables and matrices based on the data collected:

1. Asset, Threats, and Control Definitions
2. Asset Values, Threat Probability and Severity, Control Costs
3. Asset-Threat and Threat-Control Impacts

Compute the values of the assets and then find relative associations between assets-threats and threats-controls. You will need to figure out the impacts and probabilities based on the information you can gather from co-workers or other sources to come up with the best estimates possible. Remember that this information should not be the average of opinions, but a result of consensus. Make sure to write the reasoning behind the values you came up with similar to the case presented. Use the methodology in the lecture notes (and recommended readings) to cascade the values from one matrix to the other to compute the relative impact of different vulnerabilities, threats, and controls. You may choose any scale that you like (e.g. 0, 1, 3, 9) to reflect the associations between different parameters. Finally, compute the costs of the controls and perform a cost-benefit analysis. After performing the qualitative risk analysis, perform a quantitative analysis by filling in the matrices with the appropriate numeric data. It is not expected that you will necessarily get the most accurate data, however, make the best estimates possible based on other data (references should be listed). Compute and cascade the values from one matrix to the other. Then compute the cost of the controls and optimize the final security posture.

Please also include a 2-3 page single-spaced write-up which includes:

1. Background of Organization (including details on mission, size, etc.) and/or Topic of Risk Analysis
2. Scope of Risk Analysis
3. Resources used (positions of people, online resources, standards)
4. Challenges in obtaining information on assets, vulnerabilities, threats, and controls.
5. Detailed rationalizations for all asset values, as well as vulnerability, threat, and control probabilities and impacts. Discussions on why specific values, probabilities, or impacts were chosen.
6. Final analysis of the results and proposed security implementations

---

COURSE SCHEDULE

Unit	Topics	Readings
1	Introduction to Information Security Risk Analysis	TBD
2	Information Security Risks	TBD
3	Information Security Risks Cont'd.	TBD
4	Group Decision-Making, Consensus Building, & Psychological Factors	TBD
5	Qualitative Risk Analysis (Matrix Based Approach)	TBD
6	Qualitative Risk Analysis (Case Analysis)	TBD
7	Exam I	TBD
8	Uncertainty, Probability, and Risk	TBD
9	Probability and Statistics for Risk Analysis	TBD
10	Data Collection and Data Quality Issues	TBD
11	Fault Trees and Event Trees	TBD
12	Linking Risk Analysis and Decision Analysis	TBD
13	TBD	TBD
14	Exam II	TBD

Detailed Schedule

Week 1
Theme — Introduction to Information Security Risk Analysis
Topics — Risk, Information Security Nomenclature, Risk Assessment, Methodology, Objectives
Readings
Exercises — Case Study

Week 2
Theme — Information Security Risks
Topics — Denial of Service Attacks, Network Intrusions, Software Vulnerabilities, Malicious Code
Readings
Exercises — Examining Software Vulnerabilities

Week 3
Theme — Information Security Risks Cont'd.
Topics — Password Security, Wireless Security, Unintentional and Insider Threats
Readings
Exercises — Password Auditing Tools

Week 4	
Theme	Group Decision-Making, Consensus Building, & Psychological Factors
Topics	Group creation, different types of group decision making, how to build consensus, psychological factors affecting risk perception and decision-making
Readings	
Exercises	Short Cases
Week 5	
Theme	Qualitative Risk Analysis (Matrix Based Approach)
Topics	Determining Assets, Vulnerabilities, Threats, and Controls, Matrix-Based Approach
Readings	
Exercises	Short Cases
Week 6	
Theme	Qualitative Risk Analysis (Case Analysis)
Topics	
Readings	
Exercises	Case Study
Week 7	Exam I
Week 8	
Theme	Uncertainty, Probability, and Risk
Topics	Concept of Uncertainty, Basic Probability Theory, and Quantification of Risk.
Readings	
Exercises	Problem Solving
Week 9	
Theme	Probability and Statistics for Risk Analysis
Topics	Classical and Bayesian Statistics
Readings	
Exercises	Case Analysis
.	
Week 10	
Theme	Data Collection and Data Quality Issues
Topics	
Readings	
Exercises	Case Analysis
Week 11	
Theme	Fault Trees and Event Trees
Topics	Decision trees and influence diagrams; expected value model
Readings	
Exercises	Case Analysis
Week 12	
Theme	Linking Risk Analysis and Decision Analysis
Topics	
Readings	

Exercises	Analyzing Security Data
Week 13	
Theme	TBD
Topics	
Readings	
Exercises	Case Study
Week 14	Exam II