INF 710: Information Security Risk Assessment
University at Albany, State University of New York
Center for Information Forensics and Assurance
Fall 2005

Instructor Information
Name: Sanjay Goel
Email: goel@albany.edu
Phone: (518) 442-4925
Office Location: BA 310b
Office Hours: Monday 12:30-2:00 or by Appointment

Class Information
Time: N/A
Location: CIFA Teaching Laboratory (ES-B19)
Dates: November 7-18, 2005
Credit(s): 1
Call #: 8837
Available Lab(s): CIFA Teaching Laboratory

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 state and law enforcement agencies. Students will learn how to use a risk analysis matrix for performing both quantitative and qualitative risk analysis. As a part of the course the students learn of the different threats that they need to incorporate in their risk analysis matrices.

Course Format
This course is being offered as an online course. However, the intent of the course is to provide students with an interactive learning environment through instructor video, 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 2 weeks, it is important that students stay on schedule so that they can participate with other students in discussions.
The class should require approximately 40 hours of work. This should work out to roughly 15 hours of video and lecture material, 2 hour worth of quizzes, 4 hours for discussion postings, 12 hours for the final project, and 7 hours of readings.

Course Prerequisites
It is assumed that students will come in with varied backgrounds in information systems so the class will start with a general background of computer security. It would be helpful if students have some knowledge of the following topics:
- Computer Networks
- Computer Architecture
- Software Design
- Statistical and Probabilistic Analysis

Learning Objectives

Students should be able to:
- Understand the basic nomenclature and definitions of risk analysis
- Develop a work plan for executing a risk analysis in the organization
- Understand the various threats to information assets in the organization
- Identify and valuate assets
- Determine exploitable vulnerabilities
- Determine threats to an organizational system
- Recommend controls to mitigate risk

- Aggregate the data qualitatively and quantitatively to perform risk analysis

Reference Books
Please check the NIST and CERT web sites for information on risk analysis. The following books would be good references as well.

Reference: Security In Computing (3rd Ed.) by Charles P. Pfleeger & Shari Lawrence Pfleeger
Reference: Hackers Beware by Eric Cole

Additional readings will be made available via http://eres.ulib.albany.edu. The password will be made available via WebCT.

Grading
Quizzes: 20%
Discussion Postings: 30%
Project: 50%

Quizzes
Please work individually on all quizzes. A quiz will be offered after each Unit is completed through a link.

Discussion Postings
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. Discussion postings will generally be due on Wednesday and a response to someone else's posting should be up by the Sunday of that week.

Project
The students will get a take home project at the end of the class on the second day that they need to complete and submit via email to the instructor.
The end of semester project involves the use of both qualitative and quantitative risk analysis methodologies described within the lecture. 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 three matrices based on the qualitative data collected:

- Asset & Vulnerabilities
- Vulnerabilities & Threats
- Threats & Controls

Compute the values of the assets for the asset-vulnerability matrix and then find relative associations between assets-vulnerabilities, vulnerabilities-threats, and threat-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 should be 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.