



COURSE SYLLABUS

Course Name: IA 202:
Risk – Vulnerability Analysis

Instructor: Gerald V. “Skip” Lawver

Office Hours: 9:00 to 5:00 Mon-Fri

Office: Telephone: 487-3170

Internet/E-Mail Address: Skip.Lawver@emich.edu

Course Description: Tools, techniques, and methodologies in performing computer system and network security vulnerability - risk analyses. Security Best Practices and audit requirements for specific environments will be studied. Topics to be covered include internal and external penetration tests, wireless security technology, risk analysis methodology, and security audits.

Purpose: The purpose of this course is to provide undergraduate level students with an educational experience in the application of risk management theory and principles to information security policy, information systems computer and network facilities, and the life cycle development process.

Scope: The scope of the material to be covered includes:

- Risk analysis methodology, the fundamental theory of risk.
- Development of information security policy and programs based on a risk analysis approach;
- Application of risk analysis methodologies as they apply to the information systems field, and;

Course Objectives: This course will assist students in their career preparation as information system security managers. Upon successful completion of this course, students should be able to:

1. Demonstrate risk management and risk analysis
2. Demonstrate vulnerability assessment techniques
3. Demonstrate threat analysis techniques
4. Plan vulnerability assessment, threat assessment and risk analysis projects
5. Apply risk management principles throughout the software and systems development life cycles to include continuity.
6. Demonstrate Incident Handling, Continuity, and Disaster Recovery techniques
7. Define Network Security assessment and Accreditation techniques

Required Texts and Handouts: Students will receive reading assignments that may include handout material, and/or research searches, and is responsible to read and act on the material as directed. The required texts are:

- Primary Text: Information Assurance: Managing Organizational IT Security Risks, Boyce and Jennings, Butterworth Heinemann, 2002, ISBN# 0-7506-7327-3.
- Supplementary text: Enterprise Security – the Manager’s Defense Guide Clark, David Leon pub Addison Wesley, Part 4
- Various handouts as determined by your instructor

Course Content and Schedule: This schedule is an approximate timeline for the student.

Unit 1: INTRODUCTION AND RISK MANAGEMENT

Chapter 1 - 4

1.1 Introduction and Risk Management

- 1.1.1 Introductions
- 1.1.2 Course Review and Intro
- 1.1.3 Overview of the risk management process
- 1.1.4 Cost/Benefit Analysis of Information Assurance
- 1.1.5 Documentation
- 1.1.6 Risk
- 1.1.7 Risk Assessment
- 1.1.8 Risk Management
- 1.1.9 Residual Risk
- 1.1.10 Risk Acceptance Process
- 1.1.11 Systems Security Authorization Agreements (SSAA)

Unit 2: THREATS

Chapter 5

2.1 Threats

- 2.1.1 Vulnerability management
- 2.1.2 Introduction to vulnerability analysis
- 2.1.3 Attacks
- 2.1.4 Environmental/Natural Threats
- 2.1.5 Human Threats
- 2.1.6 Theft
- 2.1.7 Threat
- 2.1.8 Threat Analysis
- 2.1.9 Threat Assessment

Unit 3: VULNERABILITIES

Chapter 5 & 8

3.1 Vulnerabilities

- 3.1.1 Building a secure organization

- 3.1.2 Evaluating strong authentication methods
- 3.1.3 Vulnerabilities
- 3.1.4 Vulnerability Analysis
- 3.1.5 Network Vulnerabilities
- 3.1.6 Technical Vulnerabilities

Unit 4: ATTACKS AND COUNTERMEASURES

Chapter 8

- 4.1 Attacks and Countermeasures
 - 4.1.1 Information warfare
 - 4.1.2 Penetrating computing systems
 - 4.1.3 Malicious code
 - 4.1.4 Types of attacks
 - 4.1.5 Education, Training, and Awareness as Countermeasures
 - 4.1.6 Procedural Countermeasures
 - 4.1.7 Technical Countermeasures

Unit 5: INCIDENT HANDLING AND RESPONSE

Chapter 15

- 5.1 Incident Handling and Response
 - 5.1.1 Vulnerability assessment tools
 - 5.1.2 Planning vulnerability and penetration tests
 - 5.1.3 Monitoring vulnerability and penetration tests
 - 5.1.4 Emergency Destruction Procedures
 - 5.1.5 Organizational/Agency Information Assurance Emergency Response Teams

Unit 6: DISASTER RECOVERY AND CONTINUITY OF OPERATIONS

Chapter 12

- 6.1 Disaster Recovery and Continuity of Operations
 - 6.1.1 Business Recovery - Importance
 - 6.1.2 Contingency/Continuity of Operations Planning
 - 6.1.2.1 Establishment and testing of contingency/continuity of operations plans
 - 6.1.3 Disaster Recovery
 - 6.1.4 Disaster Recovery Plan
 - 6.1.4.1 Establish and test disaster recovery plan
 - 6.1.5 Incident response policies
 - 6.1.6 Law enforcement interfaces/policies
 - 6.1.7 Reconstitution – principles and importance of
 - 6.1.8 Restoration

Unit 7: CRITICALITY AND SENSITIVITY OF INFORMATION AND SYSTEMS

Chapter 4

- 7.1 Criticality and Sensitivity of Information Systems
 - 7.1.1 Aggregation
 - 7.1.2 Disclosure of Classified/Sensitive Information

Unit 8: DEFINING NETWORK SECURITY AND ACCREDITATION OF SYSTEMS

Chapter 8 and 11 and handout material

8.1 Defining Network Security and Accreditation of Systems

8.1.1 Memoranda of Understanding/Agreement (MOU/MOA)

8.1.1.2 Facilitate development and execution of MOU/MOA

Assignment: Develop MOU/MOA

8.1.2 Connectivity (interconnected organizations)

8.1.3 Emissions Security (EMSEC) and TEMPEST

8.1.4 Wireless Technology (electronic emanations, threats from electronic emanations)

Assessment and Evaluation: The final grade for the class will be based on the following requirements as directed by your instructor:

- Team based development, presentation and evaluation of a final project, including a complete bibliography and areas of further research, as well as a Team Leaders evaluation of each group member individually, will account for 25% of each student's grade.
- Written examinations. 50%
- Student participation in class activities will account for 25% of each student's grade. This includes attendance which is required.

All points are cumulated, converted to percent form, and converted to letter grades based on this straight scale: 94% and above, A; 90% and above A-; 87% and above, B+; 84% and above, B; 80% and above, B-; 77% and above, C+; 74% and above, C; 70% and above, C-; 67% and above, D+; 64% and above, D; 60% and above, D-; below 60%, E.

Notes on Requirements and Grading:

- Class sessions will involve interactive approach and student activities. Students are expected to have textbooks and other assigned materials with them. Students should not expect to excuse lack of participation because they did not have their textbooks, or other misc. materials including disks, or backup files (in case a file is lost or damaged).

Attendance at all times is required of all students, and failure to attend is considered lack of participation. Verifiable emergencies will only be considered.

General Policies:

- Attendance and punctuality is mandatory. Class will start at the given time.
- All cell phones, pagers and any other miscellaneous forms of communication must be turned off prior to the start of class and remain turned off until after class is completed. This is out of courtesy for the other students and to insure an uninterrupted class.
- Speak to the instructor as needed.

- Students should comply with expectations for use of the college and university laboratories and classrooms, with standards for fair information practices, and with licensing provisions of the software in use.
- Students must complete their own work when given an individual assignment. During team-based assignments they will work with one another to solve problems and develop the team-based project. Students who submit the work of other students, including companies and organizations, as their own (Plagiarism), will be penalized to the full extent permitted by University policy.
- Late work is not accepted. Oral presentations may not be made up.
- Inability to prepare for an assignment and poor time management are not considered valid reasons for late work or re-scheduling. In addition, students must back up work, for lost disks or damaged files is not sufficient reason for extensions.
- Class sessions may involve some lecture, Caucus/Online, with mostly group-facilitated activities. Therefore, it is the student's responsibility to have completed the scheduled reading assignment prior to the class session. The student must also complete the assigned chapter activities/projects during scheduled class sessions. Active listening is also part of learning. Students are expected to have textbooks and other needed materials with them. Students should not expect to excuse lack of participation because they did not have their textbooks, and/or other materials.
- Be prepared to conduct discussions online through Caucus or another form of online viewing such as e-mail.
- Students are expected to complete all assignments in a neat, accurate and professional manner; otherwise, materials will not be accepted. This includes the word processing of all assignments with spell checking and proofreading mandatory. This also includes stapling your materials if needed so they do not become loose.
- All assignments will be graded for compliance to the author's directions.
- Final grades will not be given in person, by telephone, e-mail, fax or any other communications median except that of University standard written grading at the end of the semester.
- Attendance/participation is required therefore it is the student's responsibility to obtain all missed instruction from another class member. The instructor will not repeat instructions or demonstrations for any student missing class. Keep in mind that attendance is mandatory.
- A grade of "I" will be given only in accordance with Eastern Michigan University's Undergraduate school guideline.
- By University policy the instructor has the option of failing a student who does not attend class on the day of the final examination set by the university. Attendance at final periods during which students are presenting their work is required of all students and failure to attend is considered lack of participation.

Overview of the Semester Project:

Grading: There are 40 points for the semester project and presentation.

There are 60 points for participation in class activities, assignments and exams.

More on Planning the Project:

Each team will develop a professional word-processed document (no handwritten information will be accepted), with Tabs being used to identify chapters, topics etc. and focusing on Risk Analysis and Risk Assessment, which will be presented using PowerPoint, and will at minimum include the following:

- Cover page with all Team Members Names, etc.
- Table of contents
- Names of Team members and their individual responsibilities
- The Team Leader is responsible for submitting each team member's participation and contributions to the project, which is to be included in the final document package.
- Statement of the problem. What are the issues you are dealing with and why.
- Summary statement focusing on the organization.
- Solution Statement: How will you deal with the problems, issues, etc.
- Bibliography
- Areas of further research, including a preliminary research proposal on a significant information security problem related to Risk Analysis and/or Risk Management.

The focus of the final project will be determined at the start of each term.

You will need to use NON-CONFIDENTIAL data for your project. Please do not UNDER ANY CIRCUMSTANCES use data that would breach any confidentiality. Fictitious companies and or organizations will only be used.

Final Project Documentation: A complete project with two hard (paper) copies being submitted as a total business document. Including a copy of the PowerPoint presentation. All documents must be secured in a Lightweight (paper) binder.

Academic Dishonesty

In any university-level course, a statement of policy recognizing academic dishonesty should be unnecessary. However, it should be noted that the policy of the Department of Business and Technology Education is that, any student found to have engaged in any activity constituting academic dishonesty, will receive an "E" for the course in which the activity occurred. This policy relates to all forms of work associated with the course requirements; including examinations, quizzes, laboratory work, and all other assignments. It is the student's responsibility to review the page(s) of the graduate catalog in order to determine those activities, which constitute academic dishonesty at Eastern Michigan University, which include both cheating and plagiarism. This policy will be strictly enforced.

Signature: _____

Date: _____

Course and Section # _____

- Amper, Sudhanshu Kairab, & Mattia, P.C.(2004), *A Practical Guide to Security Assessments*, Auerbach Publications
- Anthony, E.J., & Cohler, B.J. (Eds.). (1987). *The invulnerable child*. New York: Guildford Press.
- Bodin, L., L. A. Gordon and M. P. Loeb, (2005). *Evaluating Information Security Investments Using the Analytic Hierarchy Process*, Communications of the ACM.
- Gordon, L. A., M. P. Loeb and W. Lucyshyn, (2003) *Sharing Information on Computer Systems Security: An Economic Analysis*, *Journal of Accounting and Public Policy*, Vol. 22, No. 6.
- Campbell, K., L.A. Gordon, M. P. Loeb and L. Zhou, (2003) *The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market*, *Journal of Computer Security*, Vol. 11, No. 3, 2003
- Gordon, L A., M. P. Loeb and W. Lucyshyn, (2003) *Information Security Expenditures and Real Options: A Wait-and-See Approach*, *Computer Security Journal*, Vol. 19, No. 2,
- Gordon, L. A., M. P. Loeb and T. Sohail, (2003) *A Framework for Using Insurance for Cyber Risk Management*, Communications of the ACM.
- Gordon, L. A. and M. P. Loeb, (202) *The Economics Information Security Investment*, ACM Transactions on Information and System Security
- Gordon, L. A. and M. P. Loeb, (2002) *Return on Information Security Investments: Myths vs. Reality*, Strategic Finance.
- Gordon, L. A. and M. P. Loeb, (2001) *Economic Aspects of Information Security*, Tech Trends Notes.
- Gordon, L. A. and M. P. Loeb, (2001) *A Framework for Using Information Security as a Response to Competitor Analysis Systems*, Communications of the ACM.
- Gordon, L. A. and M. P. Loeb, (2003) *Expenditures on Competitor Analysis and Information Security: A Management Accounting Perspective in Management Accounting in the Digital Economy*, Oxford University Press, A. Bhimini (ed.)
- Landoll, Douglas J. (2005), *The Security Risk Assessment Handbook*, Veridyn Inc., Austin, Texas,

Peltier, Thomas R. (2005) *Information Security Risk Analysis*, (2nd), Auerbach Publication.

Tipton, Harold F., (2003). *Information Security Management Handbook*, (5th ed.), HFT Associates, Villa Park California.