

Course	ITM 5600 – Information and Communications Security
Term	Spring 1, 2010 – Saturday #1 – 8:00am – 5:00 pm 1/2, 1/16, 1/30, 2/13, & 2/27 (8am - Noon)
Instructor	Name: Don Rahn Cell: 904-485-0829 Email: dwrahn@gmail.com , Don_rahm@adp.com
Catalog Description	This course focuses on the analysis and management of information and information systems security including processes, technology, and facilities.
Prerequisites	ITM 5000 – Information Technology Management - Overview
Course Level Learning Outcomes	<p>After completing this course, students will:</p> <ul style="list-style-type: none"> • <i>know and explain the important technical and management terminology, concepts, principles, techniques, and theories related to the technical aspects of information and communications security management.</i> • <i>be able to effectively apply important technical and management concepts, principles, practices, techniques, and theories needed to critically analyze an organization’s information and communications security requirements.</i> • <i>be able to effectively apply important technical and management concepts, principles, practices, techniques, and theories needed to design and recommend appropriate security solutions.</i> • <i>be able to effectively apply important technical and management concepts, principles, practices, techniques, and theories needed to manage the implementation and on-going administration of recommended security solutions.</i>
Materials	<p>Whitman, M.E. and Mattord, H.J. (2007). <u><i>Management of Information Security</i></u>. (2nd Edition). Thomson Delmar Learning. ISBN# 1-423-90130-4</p> <p>Harris, Shon (2008). <u><i>CISSP: All-in-One Exam Guide</i></u>. (4th Edition). McGraw-Hill/Osborne. ISBN# 9780071497879</p>

Grading	<table border="0" style="width: 100%;"> <thead> <tr> <th style="text-align: left;">Assignments</th> <th style="text-align: right;">Maximum Points</th> </tr> </thead> <tbody> <tr> <td>• Final Project Presentation</td> <td></td> </tr> <tr> <td> ○ Project Presentation</td> <td style="text-align: right;">20 Points</td> </tr> <tr> <td> ○ Written project submission</td> <td style="text-align: right;">25 Points</td> </tr> <tr> <td>• Mid-term Examination</td> <td style="text-align: right;">20 Points</td> </tr> <tr> <td>• In-Class Projects and Presentations</td> <td style="text-align: right;">25 Points</td> </tr> <tr> <td>• Class Participation and Attendance</td> <td style="text-align: right;"><u>10 Points</u></td> </tr> <tr> <td>TOTAL</td> <td style="text-align: right;">100 Points</td> </tr> </tbody> </table>	Assignments	Maximum Points	• Final Project Presentation		○ Project Presentation	20 Points	○ Written project submission	25 Points	• Mid-term Examination	20 Points	• In-Class Projects and Presentations	25 Points	• Class Participation and Attendance	<u>10 Points</u>	TOTAL	100 Points
Assignments	Maximum Points																
• Final Project Presentation																	
○ Project Presentation	20 Points																
○ Written project submission	25 Points																
• Mid-term Examination	20 Points																
• In-Class Projects and Presentations	25 Points																
• Class Participation and Attendance	<u>10 Points</u>																
TOTAL	100 Points																
Activities	<ul style="list-style-type: none"> • Short lectures used to convey an understanding of mandatory topics. • Facilitated discussion of assigned readings. • Moderately complex cases, exercises, and group project assignments used to promote analysis, understanding and application of concepts and practices covered. • Final Project to promote development of research skills. • Mid-term exam to assess comprehension of theoretical concepts. 																
Policy Statements: University Policies	<p>University policies are provided in the current course catalog and course schedules. They are also available on the university website. This class is governed by the university's published policies. The following policies are of particular interest:</p> <p>Academic Honesty The university is committed to high standards of academic honesty. Students will be held responsible for violations of these standards. Please refer to the university's academic honesty policies for a definition of academic dishonesty and potential disciplinary actions associated with it.</p> <p>Drops and Withdrawals Please be aware that, should you choose to drop or withdraw from this course, the date on which you notify the university of your decision will determine the amount of tuition refund you receive. Please refer to the university policies on drops and withdrawals (published elsewhere) to find out what the deadlines are for dropping a course with a full refund and for withdrawing from a course with a partial refund.</p> <p>Special Services If you have registered as a student with a documented disability and are entitled to classroom or testing accommodations, please inform the instructor at the beginning of the course of the accommodations you will require in this class so that these can be provided.</p> <p>Disturbances Since every student is entitled to full participation in class without interruption, disruption of class by inconsiderate behavior is not acceptable. Students are expected to treat the instructor and other students with dignity and respect, especially in cases where a diversity of opinion arises. Students who engage in disruptive behavior are subject to disciplinary action, including removal from the course.</p> <p>Student Assignments Retained From time to time, student assignments or projects will be retained by The Department for the purpose of academic assessment. In every case, should the assignment or</p>																

	<p>project be shared outside the academic Department, the student's name and all identifying information about that student will be redacted from the assignment or project.</p> <p>Contact Hours for this Course It is essential that all classes meet for the full instructional time as scheduled. A class cannot be shortened in length. If a class session is cancelled for any reason, it must be rescheduled.</p>
<p>Course Policies</p>	<p>Attendance at all class sessions is expected.</p> <p>Late assignments will be accepted if prior arrangements have been made with the instructor, but will be given reduced points based upon the number of class sessions it is late.</p>
<p>Weekly Schedule</p>	<p>Pre-Assignments for Sessions 1 & 2: IMPORTANT. THIS ASSIGNMENT IS DUE THE DAY OF THE FIRST CLASS.</p> <ul style="list-style-type: none"> • Prior to the first meeting prepare a three-page paper on what you believe to be the most important part of Information and Communications Security and explain the rationale. This paper must have a Power Point presentation to go along with it for presentation. The presentation should take approximately 15 but not more than 20 minutes. • Reading Assignment: <ul style="list-style-type: none"> ○ Textbook MIS Chapters 9 & 10 ○ Textbook CISSP Chapter 2 & 7 <p>ALL READING ASSIGNMENTS AND THE TEXTBOOK SECTION ASSIGNMENTS ARE REQUIRED TO BE READ PRIOR TO THE CLASS DISCUSSION.</p>

Week 1

AM Session 8-Noon

THEME: Physical Security and Security Trends

Topics:

- Review syllabus and class format
- Assignment of Individual Projects, Current Event Discussions and Final Project Teams
 - **Please note that for the remainder of the class's current events discussions will be an integral part of the class. This information will be calculated into your individual and group grades.**
- Current Events – CERT, SANS, Trade Publications
- Organizational Policy
- Perimeter Security
- Physical Security Concepts
- Hacking/Attacks
- Pre-assignment Discussion and Presentations

PM Session 1-5

THEME: Network Security

Topics:

- Current Events – CERT, SANS, Trade Publications
- Basic Network Design and Operation
- Trusted and Untrusted Networks
- Intrusion Detection
- Extranets, DMZ
- Firewall Infrastructure Architecture

Assignments for Week 2:

- Read: Textbook CISSP Chapters 11 & 12
- Read: Textbook MIS Chapters 7 & 8
- Read and Prepare for Current Events - CERT Advisories, SANS Reports, Trade Publications
- Prepare for Individual Project Presentation
- Prepare a 1 page summary of an article covering a security topic related to the current week's reading

Week 2

AM Session 8-Noon

THEME: Network Security

Topics:

- Current Events - CERT, SANS, Trade Publications
- Protocols
- Remote Access Solutions
- Risk Identification/Assessment
- Access Controls
- Individual Class Presentations

PM Session 1-5

THEME: Server Security and Vulnerabilities

Topics:

- Current Events - CERT, SANS, Trade Publications
- Risk Control Strategies
- Server and Database Security
- Patch Management
- Web Security
- Individual Class Presentations

Assignments for Week 3:

- Review: Textbook CISSP Chapter 11/12
- Review: Textbook MIS Chapter 9 – Protecting Mechanisms
- Read: Textbook CISSP Chapter 8 - Cryptography
- Read and Prepare for Current Events - CERT Advisories, SANS Reports, Trade Publications
- Prepare Individual Class Project presentations
- Prepare to submit Mid-term examination

Week 3

AM Session 8-Noon

THEME: Vulnerability Assessments

Topics:

- Current Events - CERT, SANS, Trade Publications
- Vulnerabilities & Vulnerability Assessments
- Internet Scanner Testing
- Intrusion Detection Systems
- Individual Class Project presentations
- Mid-term due - Submittal

PM Session 1-5

THEME: Cryptography and Encryption

Topics:

- Current Events - CERT, SANS, Trade Publications
- Public and Private Keys
- PGP
- Clipper Chip
- SSL/TLS
- Link Encryption

Assignments for Week 4:

- Read: Textbook CISSP Chapters 3 & 9
- Read: Textbook MIS Chapters 4 & 5
- Read and Prepare for Current Events - CERT Advisories, SANS Reports, ZD-Net
- Prepare a 1 page summary of an article covering a security topic related to the current week's reading
- Prepare for Final Team Presentation

Week 4

AM Session 8-Noon

THEME: Business Continuity and Disaster Planning

Topics:

- Current Events - CERT, SANS, Trade Publications
- Business Continuity
- Disaster Planning
- Discuss Team Project Proposed Solutions

PM Session 1-5

THEME: Info Security Management and Policy

Topics:

- Security Controls
- Security Model and Policies
- Layers of Responsibility
- Security Training
- Current Events – CERT, SANS, Trade Publications
- Integration and Review of Course Concepts
- Review Team Project Progress – Final Project

Assignments for Week 5:

- Read: Textbook CISSP Chapter 10 – Legal
- Read: Textbook MIS Chapter 11 – Law and Ethics
- Finish Preparation of Final Team Project

	<p><u>Week 5</u></p> <p>AM Session 8-Noon THEME: Laws, Ethics and Final Presentations Topics:</p> <ul style="list-style-type: none"> • Ethics • Forensics • Cybercrime • Final Team Presentation and Critique of Presentation • Wrap-up and Review • Class Critique and Final Grades • Observations and Suggestions <hr/> <p>NOTE: Due to time constraints of this course and the amount of material to be covered, it is not possible to have in-detail coverage of all the text material. However, students should be aware that they are responsible for all text and other material. In addition, the syllabus should be considered "general guidance" for the course and, if required, the instructor can amend it.</p>
<p>Additional Information</p>	<p>Determination of Grades is Based on the Following Criteria:</p> <p><u>Minimum Requirements:</u> Products (papers, case studies, projects) must be on time, in the correct format, corrected for spelling and grammar, appropriate materials included and referenced to-the-point and on topic and conclusions must be supported.</p> <p>Examinations must be complete, accurate, neat, evidence clear thought, and exhibit concise and to-the-point responses.</p> <p>Behavior in class discussions and group activities should be responsible, should exhibit open communication, be constructive, and helpful.</p> <p><u>Mastery Level (Grade of “B”): Professional Achievement</u> Products must meet the requirements stated above for minimum requirements and additionally meet professional criteria. For example, documentation should be included to support research papers, the APA format should be used consistently throughout the paper, and substantially more than the minimum number of references should be included. Presentations should be logical, organized, and comprehensive.</p> <p>Examinations should be organized, in depth, comprehensive, logical and complete, and evidence thorough understanding of the subject /topic through application of principles.</p> <p>Classroom behavior should exhibit very focused activity and thought on the subject at hand, be motivated, and assist in discovery of new insights and relationships concerning the subject/topic of discussion.</p> <p><u>Mastery Level Plus (Grade of “A”): Creative Achievement</u> Products must meet all requirements stated above and additionally meet creative criteria. These criteria include unique topic or subject selection,</p>

	<p>synthesis of ideas, evaluation of subject matter and positions found in the literature, be creative in approach, establish new relationships with ideas and provide new insights.</p> <p>Examination responses indicate insightfulness of understanding, a synthesis of information and unique ideas, and rationale for application of principles following careful analysis.</p> <p>Classroom behavior should exhibit very focused activity and thought on the subject at hand, be motivated, and assist in discovery of new insights and relationships concerning the subject/topic of discussion.</p> <p>The grade of “A” represents the best work of students, accomplished in a unique and professional manner.</p> <p>Note:</p> <p>To achieve the objectives of this course, this syllabus may be revised at the discretion of the instructor without prior notification or consent of the students.</p>
<p>Reviewed by: <u> <i>J. Ewing</i> </u></p> <p>Job Title: <u> Faculty Coordinator </u></p> <p>Date: <u> 05/13/09 </u></p>	

Revised 05/10/09

Individual Projects, Mid-term, Final Team Project

Instructor will review the following in class

General Rules and Guidelines:

- Learning to be successful must be FUN.
- If you are not having fun with these exercises you may be approaching them from a far too granular view.
- All presentations must be in Power Point.
 - All references must be fully defined as shown in the Research Paper Guideline.
 - All presentations require two hard copies.
 - The instructor will retain one hard copy.
 - The student will have the 2nd hard copy returned after the presentation with the grade. The student will have the 1st hard copy and the soft copy for presentation purposes.
 - A student will fail if they exclusively read the presentation notes and or the actual slides.
 - If the instructor detects this reading he has the right to ask for the notes and or turn off the monitor.
 - The purpose of the presentations is stated above and this approach is used to better build these abilities.
- All the topics have more information available than the presentation time will allow.
 - The student is thus required to filter to what they deem important and what is less important.
 - All topics **MUST** be approached from a cost/benefit and risk management perspective.
- All presentations will be planned for a 20-minute window. Questions and answers can and will occur during the presentation.
 - The students will be advised in the first class session what individual project they have been assigned and when it is to be given.
- Rule of thumb for good presentations.
 - 15 slides per hour
 - No more than one topic per slide
 - No more than 6 lines per slide
 - Limit Animation and sound
 - Slide are outline points for the speaker to talk from, not the total amount of information to be presented.

Individual Projects

1. Information Security Users Policy - Discuss and present a good well thought out Information Security Users Policy. What should the policy cover? Consider software, files, virus detection, and theft of data, disclosure of data and the protection of other resources.
2. "Rainbow Series" - The Federal Guideline for Information Security has what is known as the "Rainbow Series". In this series they define Computer Security in terms of C1, C2, B1, B2, and B3. What is this in plain English? Define in English what each of these designation means.
3. ALE Model - Discuss the ALE (Annual Loss Expectancy) model and how it can be applied to Information Security. What is it? How does it apply to information security? Does it work? Is it better than intuitive thinking?
4. Denial of Service Attacks (DOS) - What is the impact to the user populations from DOS attacks that have taken place on Yahoo, E-Bay etc? How did these attacks originate, what are their unique characteristics, and how can they be prevented? What is Distributed Denial of Service Attacks (DDOS)?
5. Attacks against Windows 2000 or 2003 Server - Develop a presentation that explains how to defeat (step-by-step) the security established by Microsoft Server. What are several different approaches? How do these work? What could be done once this has been completed? What damage could be done? How can NT be protected from this? What are current vulnerabilities to NT?
6. Windows 2000 or 2003 Server Vulnerability Assessment - Develop a process to audit 2002 or 2003 to validate that all the security safe guards have not been by-passed. What could you do to ensure that it is C2? What could you do to for all servers periodically? Do products exist that would help to automate the process? Can it be done manually?
7. Data Integrity and Hacking - Present, define and describe differences between a Computer Virus, Worm, Trojan, Salami Slice, Data Diddling and other similar attacks. Give examples of each and state if they can occur from internal users, external vandals, or both.
8. Cryptography and Encryption - How does encryption work and how would we use it? What is Cryptography and Encryption? What are DES, Triple DES, and RSA? What are Public and Private Keys? What are symmetric and asymmetric Keys? Why is PKI a blessing or a failure point?
9. Authentication and Authorization - Define and describe the difference between authentication, authorization and the use of tokens. How do these they apply to Computer Security? What administrative rules should be used to make these processes more secure? What are some vulnerabilities associated with them?
10. Encryption Export - What is the current U.S. Government law on the Export of Encryption? Under what set of laws is this controlled? As of 2/25/00 what was the law, how does it compare to

today's law? What are the requirements to export what the U.S. Government calls "high encryption"?

11. TCP/IP protocol suite - In general, what is TCP/IP and how does it work? What are the layers in this protocol and what part of security can be associated with each? How does it relate to the OSI Model?
12. Firewalls - What are the various forms of Firewalls and what are the strengths and weaknesses of each? Do not work this by brand, do this by type of firewall. Is a Router a Firewall?
13. IP Spoofing - What is IP Spoofing and how is it accomplished?
14. SSL and HTTPS - What are SSL and HTTPS? How do you know when each is being used and what are the advantages and disadvantages of each?
15. ECommerce - What is eCommerce and is it hype or fact? What additional Security Risks are associated with eCommerce and how can they be best mitigated?
16. E-Mail Use - Should a Company be concerned about e-mail that is being sent by its employees from the business? What safeguards should be put in place to mitigate this risk? In the U.S. by law who is the owner of the company e-mail system and its contents?
17. Internet Use - What is the cost of Internet connection to an U.S. business today? Is there a loss to productivity as a result of this "surfing"? What cost/benefit trade-offs exist?
18. Passwords - Design and develop a process for excellent password building. Cover issues of:
 - Password aging
 - Password content
 - Password sharing
 - Password re-use
 - Others, as you deem necessary
19. Data Center Protection - Design and develop an "hardening process" for a Data Center that is based in Florida today. What unique Disaster Recovery issues present themselves as a result of the location?
20. Network Concepts - From a management standpoint explain and discuss what a network is. Use the following as a guide. What is a LAN and how is it different from a WAN? What are routers, what do they do and why are they important? What do servers do and what are the different types of servers? What are protocols and what is the OSI model? What is the difference between physical connectivity and logical connectivity? How do these relate to Information Security? Include a basic network diagram to explain these elements.
21. Information Classification – Discuss the concept of Information Classification. Does the classification of information matter? What are different methods of classification? What should result from this classification?

22. Wireless Networking – Discuss the concepts of wireless networking. What is the effect on information security? Can wireless networking be effectively managed from a security standpoint? What are some of the pitfalls in wireless technology?
23. Computer Crime – Discuss computer crime and provide examples of significant crimes and the outcomes of these crimes. Is computer crime pursued effectively, consistently and is it always prosecuted? What laws are used in these investigations and prosecutions? What is the effect of the internet, international policies, international law and access to the US from other countries?
24. Ethical Hacking – Discuss what it meant by ethical hacking. What is it? What is the difference between ethical hacking and hacking in general? Should a company hire someone that has been a known hacker?

Mid-term Examination

The mid-term will consist of a research paper that will be drawn from the following topics. The use of other topics of specific interest to students is encouraged and should be pursued. These other topics must receive the instructor's consent prior to adoption of the topic by the student. Finally, topics for the research paper may not be the same as those for individual projects and presentations. Topics for the research paper are:

Firewalls - Explore different types, applications and uses.

Firewall Architecture - Research, discuss and describe the different types of firewall infrastructures.

Encryption - Select an encryption topic and fully explore the use and purpose of encryption.

Vulnerability Scanning – provide an overview of vulnerability scanning and contrast and compare some of the products available.

Malware and Viruses – contrast and compare malware and viruses. Provide an overview of their progression and what tools are used to combat these threats.

Layered Security approach – provide an overview of a layered approach to security which should include multiple components throughout the organizations infrastructure. (i.e. Gateway filtering, IDS, router filtering, etc.) What are the most recent components added to increase security within the infrastructure?

ECommerce - What is the role of eCommerce, how is it expected to grow and what role in the future is expected for this technology?

Linux - The use of this operating system has grown significantly. What are industry expectations for this product? What makes it attractive? Are there aspects that make it unattractive?

Business Continuity and Disaster Recovery Planning - What is it and why is it so important? What should be included in a plan for Business Continuity and Disaster Recovery? What is the difference between business continuity and disaster recovery?

Organizational Ethics - Should organizations have an ethics policy? What expectations should be created with a policy? What should the policy include? How should it deal with ethical issues arising in the organization?

Windows Vista - What should the industry expect from Windows Vista? Will Windows Vista be successful and why?

Information Security Policy - Why are Information Security Policies important? What have different organizations done in this area? What are rules for success?

Current Event Discussions

Current events are a major part of Information Security and each student will be asked to summarize a topic each week that related to the reading for that particular week and turn this in on the weeks requested. A student(s) may also be asked to discuss during class the topic/article they selected for that week. These can be selected from the SANS web site WWW.SANS.ORG, CERT web site WWW.CERT.ORG or other appropriate sources of information. These will be informal discussions and should present a summary of information on news, current releases, current vulnerabilities, hacking attacks (incidents) and other similar types of coverage.

Team Project

Premise:

Your team is the part of the Security Department for CreditLand, Inc. (CLI). CreditLand is a large credit card company and has 1,000 employees.

- CLI recently acquired New Company Inc. (NCI). NCI has 300 employees and these include a full complement of technical IT staff. In many cases the personnel at NCI wear many hats. The programmers and network operations do information Security. The division of duties between them is not defined but they keep the operation going. NCI has a network, various web and mainframe computers. Your team has been assembled to develop a comprehensive security plan for NCI. The NCI network diagram is attached. CLI top management would like a presentation that describes all of the security steps and areas necessary to have a secure network and environment. They are very nervous. The following facts apply to NCI.
 - Management immediately installed the circuit between CLI and NCI to facilitate the transfer of credit card information between the two companies. Information transferred includes credit card numbers along with all of the associated personal information of the cardholders.
 - Your team has prepared the following notes based on discussions with various personnel at NCI.
 - The Network team at NCI has deployed a dial-in solution that will allow all employees to dial-in as long as they have the phone numbers. Management wanted to do this to enable users to work from home. The technicians did not want to enable monitoring and logging since that would create the need for an additional server with the increase in resources.
 - Internet access is available to everyone with a browser. There is no policy to limit the use of the Internet, email, PCs and other computer resources at NCI.

- The NT Domains allow trusts and users to login once and have access to all servers and applications. NT Administration said they would require an individual to manage user ID administration.
- Test servers are not used due to cost constraints. NCI has trusted their programmers to improve profitability. The Credit Card processing information is the sole business of NCI.
- End users at NCI are very concerned with productivity. Management is very happy with their productivity, which results in improved profitability. CLI has learned that authentication varies by individual. The same practice may not be applied to all individuals.
- The Internet servers were installed to allow customers to enter credit card information so they could get cards approved on-line. This works well and has increased the number applications substantially. Applications include all of the information to get a credit card. A few customer inquiries have been received as to the privacy policy of NCI and the security of doing this on the Internet. Management is not sure how to handle this.
- Management wanted to use an NT server as a firewall and insisted, for cost reasons, that the old server Accounting retired could do the job. They had Server Operations install it as a firewall. They took the Accounting applications off and added the web pages for Internet use. It now provides web pages to the Internet users.
- Management would like you to recommend what to encrypt. Technicians have asked about databases, transmissions, and web browser connections.
- NCI Network Operations gave a network diagram to you. It is attached.
- Management is very concerned with maintaining a high level of availability to all users including Internet users, CreditLand and dial-in. Loss of these capabilities results in lost revenue.

Your team's role is:

Design a security program for the company to improve the present state of affairs. It should be justified based on cost, benefit and risk.

- The Company MUST be in the eCommerce world to be responsive to its customers.
- EFTs pays each account.
- This plan MUST cover Physical and Information Security in all aspects built on a risk model.
- You can ask the instructor, who is the owner of the company, any questions for clarity and information relating to the company's activities, or your team's charter, and you will get the information you request.
- You cannot ask the instructor how to do specific items related to the security issue of this problem. He may not give you a correct answer.

Project Presentation and Rule of Engagement:

- All members of the team will be required to give a portion of the presentation.
- A team Captain picked by the instructor, in one of the first classes, will have the ability to assign roles and responsibilities.
- The presentation will cover all the issues and topics with advantages and disadvantages for each recommendation.
- The final presentation must be a Power Point.
- Diagrams may be imported into the Power Point presentation.
- The team can fail and individual members can pass.

- Members can fail and the team can pass.
- You will have the full final class meeting to give this presentation and have it critiqued by the instructor.
- You will be giving the presentation to the Board of Directors of the Company. They are very nervous.

GOOD LUCK!!! REMEMBER LEARNING MUST BE FUN!!!!

**New Company Inc. (NCI)
Current Network
5-25-XX**

