# MIS 7233 (Online) – CRN 1842 – Fall 2010

| COURSE TITLE | MIS 7233 Network Security  
|BLACKBOARD SITE | Fall 2010 – [http://my.ltu.edu](http://my.ltu.edu) and select CRN 1842 |

| SCHEDULE | Semester start and end dates  
| | See [http://www.ltu.edu/registrars_office/calendar_final_exam.index.asp](http://www.ltu.edu/registrars_office/calendar_final_exam.index.asp) for LTU academic calendar information. See **Important Dates for FALL 2010 SEMESTER** below. |

| INSTRUCTOR | Dr. Kamal Kakish  
| | Adjunct Professor, Graduate College of Management  
| | Adjunct Professor, Graduate College of Engineering  
| | Course Developer, LTU Online  
| | Lawrence Technological University  
| | E-mail: profkakish@gmail.com  
| | Web: [www.ltu.edu/ltuonline](http://www.ltu.edu/ltuonline)  
| | Work Phone: 404-826-6195  
| | SkypeID: KAMALDMIT; GoogleTalk: profkakish  
| | Office Location: Online  
| | Office Hours: Monday - Saturday 9am - 9pm;  
| | Notes: Please contact me email first via e-mail. If you need to get a hold of me right away, then feel free to call at anytime. |

| LEVEL / HOURS | This course will satisfy general elective requirements for DMIT, MSIS, BSCS, MSEC, MSCE, and BSCE. Three (3) Graduate Level Credit Hours  
|PREREQUISITE | Prerequisites: Graduate level [MIS 6143](http://my.ltu.edu) Minimum Grade of C- |

| REQUIRED TEXT | (See Blackboard for additional resources)  

Supporting Texts (Optional)  

Additional Resources  

| ADDITIONAL RESOURCES | LTU Online student resources: [http://www.ltu.edu/ltuonline/](http://www.ltu.edu/ltuonline/)  
| | Technical support for using Blackboard is provided by the Helpdesk, 248.204.2330 or helpdesk@ltu.edu |

| TECHNICAL SUPPORT | Technical support for using Blackboard is provided by the Helpdesk, 248.204.2330 or helpdesk@ltu.edu |
Educational Goals

This course offers an in-depth exploration of security issues and related challenges for any organization. It is highly technical, and focuses on Information and Computer Security technologies, tools, techniques and approaches. This course addresses emerging technologies and best practices that are state-of-the-art. It can yield significant value to the student during the implementation phase of an enterprise information security plan.

The course is designed to take a deep dive in today’s technologies of computer security. It will discuss the following topics in depth:

- Cryptography
- Security Standards and Protocols
- Infrastructure Security
- Internet and Web Security
- Intrusion Detection and Prevention
- Wireless security and remote access
- Disaster Recovery and Business Continuity
- Computer Forensics
- Risk Management
- Patch Management
- Privilege Management
- Auditing
- And more

Students who attend this course will have had some background knowledge in computer networks, enterprise computer security policy, and an overall understanding for the need to implement an information security plan.

Objectives

This course is designed for students working toward a degree in MSIS, MSECE, MSCE, and other disciplines with focus on Information and Computer Security. This course may be considered as one of several courses required to satisfy that emphasis. Students can gain a greater advantage if they come into this course having had:

- An enterprise information security type course
- A data telecommunication course, or
- A networking / infrastructure course

This course is NOT intended to be an introduction to information security and assumes that the students already understand the importance of developing an enterprise information security plan and policy.

The objective of this course is to equip the students with the knowledge necessary to address tactical and strategic business issues by selecting and recommending the appropriate technologies and tools necessary to solve a business problem related to the security of information and computers.

Ideally, the student will be prepared to provide an optimal solution to a real-life information security business problem upon successful completion of this course. Understanding the pros and cons of the various technologies and techniques that are available for use in order to secure and protect intellectual
property and the infrastructures that contain it, the student should be able to apply the appropriate tools, techniques, and technologies to the situation at hand effectively.

Upon successful completion of this course, each student should have a deep understanding of both business and technical issues related to:

1. Adopting/developing and implementing information security Best Practices
2. Managing risk and protecting against network attacks and malware (DoS, spoofing, hijacking, viruses, worms, Trojan horses, zombies, logic bombs, etc)
3. Understanding various types of devices that construct the infrastructure, the variety of media that carry network signal, the diversity of storage devices, and how the use of security zones and other topologies provide network/web-based security.
4. Defending the infrastructure with techniques, technologies and approaches such as authentication, digital signatures, digital watermarking, digital certificates, public and private keys, intrusion detection, intrusion prevention, standards and protocols (PKIX/PKCS, X.509, SSL/TLS, ISAKMP, CMP, S/MIME, PGP, HTTPS, IPSec, FIPS, WTLS, WEP, ISO 17799) and cryptography
5. Understanding the vulnerabilities of Wireless LAN’s, WAN’s, Protocols and Instant Messaging, and how Remote Access methods can be effectively applied to maximize security and privacy (WAP, WTLS, WEP, AAA, VPN, SSH, Telnet, Tunneling L2TP, PPTP, IEEE 802.11, 802.1X, RADIUS, etc)
6. Hardening various operating systems, network devices, and applications (with special emphasis on e-mail transmissions), and establishing the system’s security state (baselining process)
7. Understanding hacking threats & the importance of trustworthy code
8. Securing and protecting Web Components (SSL/TLS suite, LDAP, FTP, Web Services, plug-ins, directory services, dynamic content, applets, servlets, malicious cookies, etc)
9. Incorporating security best practices into the software development process in order to prevent/minimize future/production attacks.
10. Understanding the importance of auditing, what should be audited, and how to conduct an effective and timely audit.
11. Understanding Disaster Recovery and the different strategies and alternatives that can maintain Business Continuity (of course, the subject of Disaster Recovery is so broad and diverse, and deserves to have a course on its own).
12. Applying Privilege Management using the advantages of single sign-on and other techniques
13. Understanding the rules of Computer Forensics and how various types of evidence can be used to prevent future computer crime
14. Legal and ethical aspects of network security

To pursue the course objectives effectively, students will engage in the following activities:

- Read assigned material prior to the online sessions
- Complete individual assignments and submit them on time
- Participate in online class discussions (via BB Discussion Board)
- Complete a midterm examination

Unless specifically authorized by the professor, all work assignments should be solely the student’s own individual work.

Prerequisite Skills

Students who attend this course will have had some background knowledge in computer networks, enterprise computer security policy, and an overall understanding for the need to implement an information security plan.
Instructional Methods and Course Organization

A variety of instructional methodologies are used in this course, which may include but are not limited to:

**Blackboard learning environment** – Blackboard at [my.ltu.edu](http://my.ltu.edu) contains the syllabus, all assignments, reading materials, streaming videos, narrated PowerPoint mini-lectures, podcasts, written lecture notes, chapter quizzes, links to Web resources, and discussion forums. You will submit all assignments via Blackboard, and are expected to participate regularly in discussion topics. Please take time to familiarize yourself with the organization of the Blackboard site. You will want to check the site frequently for announcements reminding you of new resources and upcoming assignments.

**Student/Instructor Conversations** – Students keep in touch with the instructor via e-mail messages, telephone conference calls, and IM conversations.

**Required readings** – Textbook chapters should be read according to the schedule outlined in the syllabus. Chapters will be discussed online.

Class Policies and Expectations

I plan to offer you a valuable learning experience, and expect us to work together to achieve this goal. Here are some general expectations regarding this course:

Each student has a LTU e-mail account. If you wish to use a different e-mail address for this course, please change your e-mail address in Blackboard under “Student Tools” and send an e-mail to me so I can store your address in my e-mail directory.

Readings, discussion forum participation, and written assignments must be completed according to the class schedule. If business travel will take you away from regular participation, please clear these dates with me in advance.

It is essential that all students actively contribute to the course objectives through their experiences and working knowledge of business and IT.

All assignments must be submitted on schedule, via Blackboard, and using Microsoft Office-compatible software. If you need to submit an assignment via e-mail, contact the instructor in advance. Late work will be reduced in value.

Assignments must be completed to an adequate standard to obtain a passing grade. Requirements for each assignment are detailed in this syllabus and on the LTU Online web site.

Be prepared to log into Blackboard at least once each day. Please focus your online correspondence within the appropriate Blackboard discussion forums so that your colleagues can learn from you.

At the end of the course, you will be invited to participate in a University evaluation of this course. Your feedback is important to the University, to LTU Online, and to me as an instructor, and I encourage you to participate in the evaluation process.

The topics listed in the syllabus are only an estimate of the material, which can be covered during the semester. Some topics might be deleted and some others might be added at the discretion of the instructor. Teamwork and collegiality are encouraged but everyone must understand and be responsible for their work, actions and work products; observations of the Honor Code Policy are mandatory. [http://www.ltu.edu/currentstudents/honor_code.asp](http://www.ltu.edu/currentstudents/honor_code.asp) All other University policies regarding incomplete grades, etc. apply.
Academic Integrity:

This course falls under the provisions of the policies on academic integrity of LTU. Any violations of this policy will result in failure. Students are encouraged to utilize the Safe Assign tool within Blackboard to insure their writings meet the provisions of this policy.

Online Participation:

Students are expected to actively participate online using the Bb Discussion Board. The due date for each discussion board posts is Sundays 11:59 p.m. of the associated chapter(s) is scheduled according to the class calendar below.

Assignments:

All assignments should be delivered electronically via the Blackboard Submission Manager/Link located under “Assignments”. If technical difficulties are encountered, you may send the assignment via e-mail to profkakish@gmail.com, but only as a last resort. Assignments are due on or before the date assigned. Late assignments will cause a 10% per day deduction from the value of the assignment.

It is important for you as students to know what to expect from me as your instructor:

1. I will be available to you via e-mail and phone, and will promptly reply to your messages, usually within 24 hours or less.
2. I will NOT be available to you for face-to-face appointments (I do not live in Michigan), but will use Wimba Live Classroom or a regular phone conference for synchronous discussions as requested.
3. I will maintain the Blackboard web site with current materials, and will resolve any content-related problems promptly as they are reported to me.
4. I will send out frequent announcements and e-mail updates to all class members to guide upcoming work and remind you of assignment due dates.
5. I will return all assignments to you promptly (usually within 72 hours of submission due date), and will include individualized comments and suggestions with each assignment.
6. I will hold our personal written or verbal communications in confidence. I will not post any of your assignments for viewing by the class without requesting your approval in advance.
7. I will treat all members of the class fairly, and will do my best to accommodate individual learning styles and special needs.

If any of these points need clarification, or when special circumstances arise that require my assistance, please contact me so that we can discuss the matter personally.
Course Schedule

This fully online course begins with a one-week online course orientation period to familiarize yourself with the online learning environment and to meet online or via phone with your instructor. Each week starts on a Monday and ends on a Sunday.

<table>
<thead>
<tr>
<th>Dates</th>
<th>Modules</th>
<th>Topics / Readings</th>
<th>Assignments Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior to Semester Start and Sep 8 – Sep 12</td>
<td>Module 0</td>
<td>Overview of textbook Online Learning Orientation</td>
<td>Bb Forums Student Data Sheets</td>
</tr>
<tr>
<td>Week of Sep 13 – Sep 19</td>
<td>Module 1</td>
<td>Chapters 1-4</td>
<td>Bb Forums</td>
</tr>
<tr>
<td>Week of Sep 20 – Sep 26</td>
<td>Module 2</td>
<td>Chapter 5</td>
<td>Bb Forums Crypto Demo – put in View/submit assignment Due by 11:59pm on 9/26</td>
</tr>
<tr>
<td>Week of Sep 27 – Oct 3</td>
<td>Module 3</td>
<td>Chapters 6, 8, 10</td>
<td>Bb Forums Public Key Infrastructure Impact of Physical Security on Network Infrastructure Security Assignment #1 Due by 11:59pm on 10/3</td>
</tr>
<tr>
<td>Week of Oct 4– Oct 10</td>
<td>Module 4</td>
<td>Chapters 7, 9</td>
<td>Bb Forums Standards and Protocols Network Fundamentals</td>
</tr>
<tr>
<td>Week of Oct 11 – Oct 17</td>
<td>Module 5</td>
<td>Chapters 11, 12</td>
<td>Bb Forums Wireless and Instant Messaging Remote Access Assignment #2 Due on 10/17 by 11:59pm</td>
</tr>
<tr>
<td>Week of Oct 18 – Oct 24</td>
<td></td>
<td><strong>Mid Term Exam</strong></td>
<td><strong>Mid Term Exam Available under Assignments Tab after 6:00 a.m. on Friday 10/22/10 to 11:30 p.m. on Sunday 10/24/10 Bb Forums Mid-Term Evaluation</strong></td>
</tr>
<tr>
<td>Week of Oct 25 – Oct 31</td>
<td>Module 6</td>
<td>Chapter 13</td>
<td>Bb Forums Intrusion Detection Systems</td>
</tr>
<tr>
<td>Week of Nov 1 – Nov 7</td>
<td>Module 7</td>
<td>Chapters 15, 18</td>
<td>Bb Forums Software Development Best Practices Assignment #3 Due on 11/7 by 11:59pm</td>
</tr>
<tr>
<td>Week of Nov 8</td>
<td>Module 8</td>
<td>Chapters 16, 17</td>
<td>Bb Forums</td>
</tr>
</tbody>
</table>
# Student Evaluation

The course has six assignments, discussion board activities, and a mid term exam totaling 100 points (left column). Letter grades are awarded based on the total number of points achieved (right column). Points are deducted for late assignments.

<table>
<thead>
<tr>
<th>Assignments</th>
<th>Points</th>
<th>Class Points</th>
<th>Letter Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto Demo Report on a Cryptography SW Package</td>
<td>50</td>
<td>95 and above</td>
<td>A</td>
</tr>
<tr>
<td>Individual Assignment 1 CISSP, Security+, SSCP, CISM, CCSP, Other Exams and CNSS, US-CERT Research Report</td>
<td>100</td>
<td>90 – 94</td>
<td>A-</td>
</tr>
<tr>
<td>Individual Assignment 2 Activity – Security Situation – Select any TWO of the 4 activities</td>
<td>100</td>
<td>87 – 89</td>
<td>B+</td>
</tr>
<tr>
<td>Individual Assignment 3 Infrastructure Security Case - Proposal</td>
<td>100</td>
<td>83 – 86</td>
<td>B</td>
</tr>
<tr>
<td>Individual Assignment 4 Intrusion Detection System</td>
<td>100</td>
<td>80 – 82</td>
<td>B-</td>
</tr>
<tr>
<td>Individual Assignment 5 Risk Management</td>
<td>100</td>
<td>77 – 79</td>
<td>C+</td>
</tr>
<tr>
<td>Midterm Exam Chapters covered to date</td>
<td>250</td>
<td>73 – 76</td>
<td>C</td>
</tr>
<tr>
<td>Online Participation Online Forum Discussions on Bb</td>
<td>200</td>
<td>70 – 72</td>
<td>C-</td>
</tr>
<tr>
<td>Total</td>
<td>1000</td>
<td>61 – 70</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>60 and below</td>
<td>E</td>
</tr>
</tbody>
</table>
Practical Guidelines for Class Load Expectations

A three-credit graduate course generally requires at least nine hours per week of time commitment. Here are some practical guidelines to help schedule your time commitments for this online course:

A 14-week semester would require at least 126 hours of time commitment to successfully complete all readings, activities, assignments, and texts as described in this syllabus.

You should reserve at least 6 hours per week to read the required textbook chapters and resources, participate in online discussions, review presentation materials, and work through online quizzes. This effort will total at least 84 hours over the course of the semester.

You should organize your remaining time to roughly correspond with the point value of each major assignment. This means that you should plan to spend at least:

- 8-9 hours preparing your case study review;
- 24-40 hours working with your group on the three parts of your semester-long project; and
- 8-9 hours working on the various components of your reflective consolidation (final exam).

These guidelines may not reflect the actual amount of outside time that you – as a unique individual with your own learning style – will need to complete the course requirements. The number of hours each week will vary based on assignment due dates, so please plan ahead to insure that you schedule your academic, work, and personal time effectively. The following graphic can be used to guide you in planning your weekly course work to remain on schedule:

<table>
<thead>
<tr>
<th>MON</th>
<th>TUES</th>
<th>WED</th>
<th>THU</th>
<th>FRI</th>
<th>SAT</th>
<th>SUN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Textbook Chapter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Take Online Chapter Quiz</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Participate in Weekly Blackboard Discussions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Individual and Group Project Work - Coordinate With Colleagues</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Instructor Communication - As Needed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Assignment Details

Course assignments and evaluation criteria are detailed below. Please review these requirements carefully. See the section Academic Resources / Assessment Guidelines for information about assessment of written and oral presentations.

Details for all assignments are shown below. Please note that you should not submit any assignments to the Blackboard “Digital Drop Box.” All assignments are submitted using the Blackboard “Assignments” function. Some assignments are also posted to the Blackboard Discussion Forum for student comments.

Crypto Demo

For this exercise, once you finish chapter 5 (Cryptography), search the internet to find a FREE demo of a Cryptographic software package of your choice (there are tons of them out there). Download and install the demo or free product on your machine and play with it. Then write a 500 word report describing the product, what protocols is uses, how it works, what you learned from it, and if you would recommend it and why. Submit your report to BB under View/submit Assignment. Also, put a PowerPoint presentation for your demo in the BB Discussion Board so other students see it. Finally take a look at what the other students submitted for their demo.

Assignment # 1
Security Certification Research
“Some certifications are hot, some not”

Security Certification has increasingly become an important consideration among business managers and technical professionals alike. With the advent of 9/11 terrorism and the progressive threats and attacks on computer and data systems worldwide, governments and businesses have sharply increased their requirements for information security certified professionals.

Students should research information on the various types and classifications of Security Certifications from a variety of sources. At minimum students should contrast, compare, and report on the following certifications:

- CISSP (from ISC2)
- CompTIA Security+
- SSCP
- CISM
- CCSP, and
- Other relevant Certifications and Exams.

Your personal observations and conclusions on certification

In addition, students should visit the Center for National Security Studies (CNSS), US-CERT http://www.us-cert.gov/, and other cyber-terrorism and counter-terrorism websites including the Whitehouse and the Department of Homeland Security (DHS), and summarize their findings, assessments, and personal opinions regarding the US readiness in combating information threats and attacks, and the degree to which Information Technology is able to address national and global information security issues.

The length of the report should be a minimum of 1,200 words but should not exceed 2,000 words, using APA style format with references (both within and at the end) and a font of “Arial 12”.
Assignment # 2
Security Scenario

For the 2\textsuperscript{nd} assignment, you may select ANY TWO of the 4 following activities – the choice is yours.
Remember: you should answer ONLY TWO of the 4 activities:

Activity 1: E-mail memo to customer regarding Melissa virus incident

Situation:

Recently, a workstation in the Engineering Department was infected with a virus delivered through e-mail. You investigate and discover that the virus did not penetrate your normal security protections, which would have detected and cleaned the e-mail arriving through the company’s mail servers. An engineer had, however, in addition to the normal company mail, established a Hotmail account and had downloaded an e-mail unaware of the virus that was attached. When the engineer opened the attachment, the virus installed itself. The Hotmail account was not being used for work purposes; however, everybody knows that employees access web mail for personal reasons on a regular basis. You need to solve the problem, and then prepare an incident report that describes the incident and what you did to resolve the problem.

Write an informal incident report as an e-mail memo to your supervisor.

In the memo, describe in your own words what happened, and the corrective action taken. The corrective action should include the steps to prevent further attacks of this kind. The steps should list how to find the virus, how to get rid of it, and finally, what you recommend the company to do about user education and policies for use of e-mail.

Criteria for Success:

At least two solutions to the problem including (1) user education and (2) the regular use of antivirus software. Your solutions will be read for reliability and effectiveness of the proposed solutions. For instance, how reliable will user education be in preventing users from using non-secure e-mail services at work? When you suggest installing and keeping antivirus software up-to-date, discuss the most reliable strategy for doing this. Finally, suggest a company policy to warn employees about the security risks of non-secure e-mail services and the possible consequences if they choose to ignore this warning.

Appropriate and correct language for the intended audience, in this case a technical audience. The language should be accurate, spell-checked, and grammatically correct.

Activity 2: Factory worker doing eBay business on company’s computer

Situation:

Acme allows employees to use their computers for personal use such as checking bank statements and personal Web searches. An employee has requested that he be able to use his laptop at work and home for checking his eBay store during lunch breaks and at home for doing other eBay activities. Your boss has asked you to study the issue and recommend a company policy regarding eBay. Determine if there are any security issues associated with eBay. Choose a position and develop pros and cons in the policy. Draft the policy in a memo format.

Criteria for Success:

Display knowledge of security issues as relevant to the requirement.
Develop position developed logically and with general security policies in mind.
Use accurate and appropriate language that is spell-checked and grammatically correct.

Activity 3: Engineer is not allowing his workstation to be updated with the most recent patches
Situation:

An engineer is not allowing his workstation to be updated with the most recent patches because the updates cause problems. His workstation is used to run large computations and many computations may run for days. Updates, especially automated patches and virus fixes, often require reboots. These unplanned reboots interrupt the computation, which forces the engineer to restart the computation from the beginning. Unscheduled reboots have direct impact on his schedule to support his projects. The results of the computations and many graphics files created are used by other engineers. They are stored in JPG format on his workstation, so his system must be on the network that exposes it to virus infections. Company security policy requires virus updates and security patches to be kept up-to-date. Explain the importance of following the Company security policy and let him know that you will be providing him a solution. Then type a memo to your manager in which you suggest three solutions with their pros and cons, and recommend the best solution.

Criteria for Success:

Memo to engineer regarding the security policies and reasons for the need to comply with the security policies.
Memo to your supervisor describing alternative plans to solve the problem.
Spell-checked and grammatically correct language.

Activity 4: A company executive is concerned about company’s confidential data being compromised

Situation:

Acme has recently begun work on a new product that requires the engineers to collaborate with another firm located in another state. In order to collaborate, the engineers are using shared design software on Acme’s server. They also plan to co-develop technical documentation, which will be stored on Acme’s server. An Acme executive is concerned that the company’s confidential data will be compromised on the project, if outsiders are allowed to access proprietary information. You have been asked to give a presentation on the security aspects of remote access and how the security procedures such as VPN and cryptography will protect Acme’s confidential information. A short PowerPoint presentation on how VPNs and cryptography will protect Acme’s network should be appropriate for Acme’s high level managers.

Criteria for Success:

Detailed information regarding VPN, how it works, and why it is more secure than a normal network.
Description of cryptographic techniques and the one, which is most secure.
A suggested solution with justifications for the solution being a best practice.
PowerPoint presentation with title page, table of contents, purpose, body, and conclusion charts.
Spell-checked and grammatically correct language.

Assignment # 3
Infrastructure Security

To complete this assignment, you need to read “Reading 2”, which can be found on page #8 in the Readings and Cases in the Management of Information Security Textbook, AND, “Case A”, which can be found on page A-1 of the same book.

Here, you are presented with a fictitious computer gaming company (CGT, Inc.) that has put out a Request for Proposal (RFP) relative to a variety of security needs and objectives that will align with and support the company’s goals, if implemented effectively.

The proposal you prepare in response to the RFP has a well-structured format that you should follow. This case study will expose you to a number of security topics, but most importantly, I’d like you to focus the bulk of your efforts on the logical and physical security design, and implementation strategies which
can be found under sections III and IV of the RFP on page A-9. These 2 sections will provide ample opportunity to leverage the Infrastructure Security knowledge you gained from chapters 6, 8, 9, 10, 17, and 18 of your main textbook – Principles of Computer Security.

Your job is to prepare and present a proposal in response to CGT’s RFP which starts on page A-7. Again, please make sure you follow the proposal format with the following exceptions:

In section I, you may skip the following items:

Feasibility Study. We will assume that the project is feasible.
Estimate of costs
Feasibility analysis

In section II, you may skip the following:

Documentation of findings and updated feasibility analysis. You should document your findings, but ignore the updated feasibility analysis.

In section III, you may skip the following:

Feasibility
Recommendation for continuing and/or outsourcing the project

In section IV, you may skip the following:

Documentation of the system
Updated feasibility analysis
Section V maybe skipped all together.
Appendix B: Copies of Pricing Sources maybe skipped in its entirety.

Assignment # 4
Intrusion Detection System

The objective of this assignment is to provide you an opportunity to do your own research in order to understand the various issues associated with recommending Intrusion Detection Systems (IDS) for a corporation.

To begin with, you received an e-mail from your boss informing you that your company has decided to invest in IDS. Your boss is asking you to interview the IT Security Manager at your place of work (if you can’t find someone to interview, you may interview a professor) for the purpose of understanding the company’s requirements for the IDS. During the interview, you must start with the business objectives then drill down to the specifics of the IDS needs. You must align the needs of implementing the IDS directly with the corporate goals and objectives regarding information security.

A logical sequence of events might flow like this:

Educate yourself all you can about IDS. Review chapter 13 in your textbook and research additional IDS topics beyond the textbook.
Compare and contrast the pros and cons of network versus host-based IDS solution. You want to make sure you understand the ins and outs of both solutions prior to the interview. You may potentially consider a hybrid solution, depending on the needs you gather from the interview.

Conduct the interview and identify the following (make sure you prepare your list of questions before you conduct the interview):
1. Business goals and objectives as they relate to information security
2. Specific corporate objectives for Intrusion Detection
3. Corporate Policy as it relates to Intrusion Detection
4. IT objectives for an IDS system
5. Security data requirements. They may include devices, topology, and intrusion detection
6. List of requirements for the ideal IDS solution
7. Criteria for selecting the appropriate IDS solution.
8. Requirements are analyzed relative to applicable time, technology, and cost constraints.

After the interview:
1. Document the requirements for the ideal IDS solution and draft a memo to the IT Security Manager to confirm your understanding of such requirements.
2. Research at least 3 IDS packaged solutions available in the market, based on the requirements and criteria provided by the IT Security Manager, and compare the pros and cons of each. This will help you finalize your decision for a recommendation. Hint: use the table below to help your research.
3. Draft a proposal to the IT Security Manager of your company explaining the following:
4. Your assessment of the company’s needs for IDS.
5. Your findings relative to the IDS available on the market. For each IDS package list the pros and cons
6. Provide your best choice recommendation
7. Defend your rational for making the best choice recommendation.

<table>
<thead>
<tr>
<th>Name</th>
<th>Product</th>
<th>Where to Find More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Systems, Inc.</td>
<td>Cisco IDS</td>
<td><a href="http://www.cisco.com">www.cisco.com</a></td>
</tr>
<tr>
<td>Computer Associates</td>
<td>eTrust</td>
<td><a href="http://www.ca.com">www.ca.com</a></td>
</tr>
<tr>
<td>Enterasys Network</td>
<td>Dragon</td>
<td><a href="http://www.enterasys.com">www.enterasys.com</a></td>
</tr>
<tr>
<td>Internet Security Systems, Inc.</td>
<td>RealSecure</td>
<td><a href="http://www.iss.net">www.iss.net</a></td>
</tr>
<tr>
<td>Intrusion, Inc.</td>
<td>SecureNet, SecureHost</td>
<td><a href="http://www.intrusion.com">www.intrusion.com</a></td>
</tr>
<tr>
<td>Intruvert Networks</td>
<td>IntruShield</td>
<td><a href="http://www.intruvert.com">www.intruvert.com</a></td>
</tr>
<tr>
<td>iPolicy Networks</td>
<td>ipEnforcer</td>
<td><a href="http://www.ipolicynetworks.com">www.ipolicynetworks.com</a></td>
</tr>
<tr>
<td>NetScreen</td>
<td>NetScreen IDP</td>
<td><a href="http://www.netscreen.com">www.netscreen.com</a></td>
</tr>
<tr>
<td>NFR Security, Inc.</td>
<td>NFR</td>
<td><a href="http://www.nfr.com">www.nfr.com</a></td>
</tr>
<tr>
<td>Snort</td>
<td>Snort (free, open source)</td>
<td><a href="http://www.snort.org">www.snort.org</a></td>
</tr>
<tr>
<td>Symantec Corporation</td>
<td>Intruder Alert</td>
<td><a href="http://www.symantec.com">www.symantec.com</a></td>
</tr>
<tr>
<td>TippingPoint Technologies</td>
<td>UnityOne</td>
<td><a href="http://www.tippingpoint.com">www.tippingpoint.com</a></td>
</tr>
<tr>
<td>Tripwire, Inc.</td>
<td>Tripwire</td>
<td><a href="http://www.tripwiresecurity.com">www.tripwiresecurity.com</a></td>
</tr>
</tbody>
</table>

Assignment # 5
Risk Management

To complete this assignment, you need to read “Reading 5”, which can be found on page #45 in the Readings and Cases in the Management of Information Security Textbook, AND, “Case B”, which can be found on page B-1 of the same book.

Here, you are presented with a fictitious government agency that is dealing a number of security issues. The case clearly identifies the risks and vulnerabilities, and discusses the recommendations for mitigating such risks.
Your job is review, assess, and debate each pair of risk/mitigation, and answer the following questions:

State the risk/vulnerability in your own words. If you had to tell the CIO about this risk during your elevator ride with him down to the cafeteria, what would you say?

In your opinion, what is the source(s) of these risks? For example, are they related to Policy or lack of it? User Education and Awareness? Technology? A combination of 2 or all of the above? Is there a single Root Cause? List as many sources/causes as you can.

State the mitigation technique for this risk in your own words, much like the same approach in the 1st question. Do you agree with the prescribed mitigation? Why/Why not? What would you suggest to improve the proposed mitigation? Can you come up with a better mitigation plan? What is your contingency plan to this mitigation plan?

Draft your report, which you will submit to your CIO, to the tune of 1,200 to 2,000 words, single space, using APA style format with references and a font of “Arial 12”.

Online Participation (20 points)
Each student is expected to actively participate in online activities. Class participation is evaluated to a maximum of 20 points based on actively participating in Blackboard discussion forums, responding to questions posted by the instructor, and interacting positively with other students.

Syllabus Addenda

Please see the LTU Online “Current Students” web site http://www.ltue.edu/ltuonline/currentonline.asp for comprehensive information about Lawrence Tech’s academic services, library services, student services, and academic integrity standards. The content of this web site is explicitly included as syllabus requirements.

The LTU Online “Current Students” web site also includes grading rubrics used by your instructor to evaluate written assignments, discussion forum participation, and group assignments. Please note that the Safe Assign anti-plagiarism product will be used for written assignments submitted for this course. Please see the instructions included on the LTU Online web site regarding the use of the Safe Assign product.

Important Dates for FALL 2010 SEMESTER
April 24 – August 24 Regular Registration
August 24 Last day to register for traditional semester courses without a late fee
August 25 Traditional semester courses begin; add/drop period begins LATE REGISTRATION FEE applies
September 5-6 Labor Day break
September 7 Classes resume
September 7 Last day to register for College of Management courses without a late fee
September 8 College of Management courses begin; add/drop period begins; LATE REGISTRATION FEE applies for College of Management courses
September 7 Last day to drop traditional semester courses with refund (no refund for classes dropped after September 7)
September 8 Withdrawal period begins for traditional courses; late transaction fee applies for each course added
September 20 Last day to drop College of Management courses with refund (no refund for classes dropped after September 20)
September 21 Withdrawal period begins for College of Management courses; late transaction fee applies for each course added
September 30 Last day to register for classes (regardless of when they start) – Traditional and College of Management courses
November 10 Last day to withdraw from College of Management courses
November 17 Last day to withdraw from traditional semester courses
November 24 Last day of classes before Thanksgiving break
November 29 Classes resume
December 11 Last day of College of Management classes before Final Exams
December 11 Last day of traditional semester classes before Final Exams
December 13 - December 18 College of Management Final Exams
December 18 Last day of College of Management semester
December 13- December 18 Traditional Semester Final Exams
December 18 Last day of Fall 2010 semester
December 22 Grades due

Please note that for courses that are start or end at times other than indicated or are of a different length, DIFFERENT dropping, adding and refund dates apply. It is the student's responsibility to be aware of these dates.