

Syllabus

The Business of Information Security
SEC 420-51
Spring Semester 2008
Champlain College

Ray Vezina, MS
Adjunct Faculty
Champlain College
Phone: (802) 316-2478
E-Mail: rvezina@vdh.state.vt.us

Course Description:

Students will learn about the management- and business-related aspects of information security, what one might think of as the "less technical" aspects of INFOSEC but ones that are critically important to successful protection of an organization's information. Rather than focus on specific information security technologies, students will examine issues related to implementing security in the larger context of an organization, such as personnel issues, computer and network policies, corporate planning, and the law.

Course Objectives:

Program Competencies	Objective
1, 2, 8, 10	Articulate the non-technical aspects of computer and network security as they relate to the larger goals of information security and day-to-day operation of an organization.
2, 6, 8, 10	Describe information security in terms of risk analysis, assessment, and avoidance.
1, 2, 5, 9, 12	Design a security assessment, audit, and vulnerability testing plan for an organization.
2, 6, 8, 9, 10, 12	Advise an organization about how to maintain compliance with relevant laws and policies related to managing and securing information.
4, 6, 7, 12	Classify the types of individuals that might threaten an organization, and devise policies and defenses for the various threat categories.
3, 6, 7, 8, 10	Describe aspects of an information security policy that are <i>not</i> related to computers and networks.

Relationship to Core Competencies:

- *Technology:* This is a course about advanced computer technology and assumes that students have already mastered the college's technology competencies.
- *Written Communication:* Students will be required to write weekly or bi-weekly reports, culminating in a research project (that requires the use of word processing technology).
- *Oral Communication:* Students will be required to orally present at least one of their weekly reports and prepare a project presentation (that requires the use of presentation graphics technology).
- *Global Studies:* The course examines legal and cultural issues well beyond North America, to study business-related issues that apply to organizations everywhere in the world and are particularly relevant to companies with a global presence. Case studies will reinforce how culture affects business decisions, including awareness about information security and privacy protection.
- *Critical & Creative Thinking:* Applying business processes to information security is a skill spanning multiple disciplines. Individuals must examine often competing claims about user and organizational demands versus regulatory and legal requirements versus security implementation capabilities and needs. The information security professional needs to optimize information security plans with the very real competing goals of an organization.
- *Quantitative Literacy:* This course examines information security from a business perspective -- e.g., risk analysis, statistical analysis, and economic analysis. Students, then, will learn to assess the business aspects of information security and analyze the numbers to determine the best course of action.
- *Ethical Reasoning:* The information security aspects of business -- as in so many other aspects of business -- come complete with ethical issues; user privacy vs. the needs of the business, corporate "spying" on users, protection of user and customer information, selecting vendors, etc. Decisions related to all of these issues must be made within an ethical context. Personal, industry, and professional ethical frameworks are presented in this course, as well as regulatory and political pressures.

General Course Policies and Procedures

Course Requirements

- 1) Active and engaged participation via discussions and collaborative group work.
- 2) Access to the Internet
- 3) Must know how to use Microsoft Power Point and Word
- 4) Demonstrate knowledge of critical issues through course homework and final course project.

Grading Policies

The grading factors are:

- Homework30%
- Class Participation30%
- Course project..... 40%

Total.....100%

Homework assignments will count for 30% of the course grade and may include essay questions requiring thoughtful response, not to exceed two pages or 500 words, unless otherwise mentioned, and will be graded on a 100 point scale. All homework assignments will be averaged to produce the final Homework score for the semester.

Class participation will count for 30% of the course grade and will be measured by participation in class. At any time after the second week of the class, students may inquire about their current Class Participation grade.

The Course Project is a semester long project designed to offer the students an opportunity to focus on a particular area of interest to student and relevant to the course subject matter. The project will be done individually. The course project is grading in accordance to the following criteria:

Contents: 70%
Presentation: 20%
References: 10%

Course project ideas must be submitted by the end of the third week of the course, however, please feel free to submit ideas and being working on the project before the third week.

All project papers are due by the end of the course. The project must be submitted in electronic form and in-class presentations must be given in the last class period of the course.

The purpose of the presentations is to inform your fellow classmates of your project and get their feedback.

Throughout the course, there will also be a number of Discussion questions. These do not require a formal response. These are only to stimulate conversation for the in-class and online discussions. Responses or comments to the discussion questions are not graded, however, class participation is graded, and therefore, all students are encouraged to add you're their thoughts to the discussions. If there are no discussion questions in a given week, the homework questions can serve to get a discussion started.

The Grading Scale will be as follows:

Points	Grade
90 – 100	A
80 – 89	B
70 – 79	C
60 – 69	D
59 and Below	F

Course Project:

The course project is grading in accordance to the following criteria:

Contents: 70%

Presentation: 20%

References: 10%

Course Textbooks:

Required:

Management of Information Security by M. Whitman & H. Mattord

Reference:

Computer Security Handbook edited by S. Bosworth & M.E. Kabay.

Defense in Depth <http://www.nsa.gov/snac/support/defenseinddepth.pdf>

Network Security http://www.nsa.gov/snac/support/sixty_minutes.pdf

Recommended: *Security Engineering* by R. Anderson.

Students should also access the information security texts available in the Miller Information Commons (MIC), as well as the online databases accessible through the library Web site at <http://library.champlain.edu>.

There are also extensive resources available from The Committee on National Security Systems (CNSS), National Information Assurance Partnership (NIAP), National Information Assurance Training and Education Center (NIATEC), National Institute of Standards and Technology (NIST), and other sources. Links to these, and other sites, can be found at <http://infosec.champlain.edu/library/> and <http://www.garykessler.net/library/securityurl.html>.

Academic Policy on Integrity:

Please review the College's Policy on Academic Integrity at the following link:

Please also review the College's Policy on Plagiarism at the following link:

There is a great deal of information on the Internet and print materials and the opportunity, willful or unintended, for plagiarism has risen substantially. Please make every effort to ensure that all work is your own. The punishment for plagiarism or any form of cheating can be severe.

Communication Policy:

Communication is critical in this course, and especially for an online course. Please be active in all class discussions and through e-mails to myself and fellow students. In addition, I strongly encourage you to respond to questions raised by fellow classmates.

For this course, please feel free raise open questions and comments regarding the course, as well as any area of security. Also, please feel free to respond to questions raised by fellow classmates.

Class Schedule:

Week	Topic	Assignment	Reading
1	Introduction Transition from IT to Management – what does an IT person need to be a successful CIO?		
2	Security Overview – Personnel, Physical, & IT		Defense in Depth, National Security Decision Directive 298
3	Security/IT Policy Creation I – this will also cover the creation of a policy enforcement capability.	Identify Security/IT Policy templates for your organization’s industry/sector. Submit Topic Ideas & Groups for Course Project.	Network Security (pp. 7-10), NIST SP 800-12 (chap. 8-10, 14, 15, 18)
4	Security/IT Policy Creation II	Identify Security/IT Policy templates for your organization’s industry/sector.	SAN’s Policy Project
5	Compliance – e.g., HIPAA, SOX, Hatch Act, GLBA, PATRIOT ACT I & II, FERPA, etc.	Identify the local, state, and Federal Laws, statutory and regulatory guidelines your firm/industry must abide by & the associated compliance enforcement body/agency.	
6	Security Awareness – now that we have a security policy, how do we make people follow it?		
7	Risk Assessment and Analysis – what is the organization’s overall risk exposure? Security Audit	Homework: What is the overlap between ‘risk’ and ‘compliance’?	NIST SP 800-12 (chap. 7), NIST SP 800-30
8	Personnel Management – a look at the unique challenges of managing IT personnel in a non-IT organization: <ul style="list-style-type: none"> • Outsourcing • What career progression can be identified for IT staff? • If IT personnel are expected to provide 24/7 remote support, why must they arrive to work by 9:00am and stay till 5:00pm? 		NIST SP 800-12 (chap. 10)
9	Communication Skills – lawyers talk legalese, management talk ‘shareholder value’, IT personnel talk techese, so how do all communicate? And how do we get our point across?		
10	ROI and Financial Planning –	Determine how your	NIST SP 800-14 , NIST SP 800-

	how to justify IT, Security projects to senior management?	organization selects, approves, plans for, finances, manages, and monitors its business projects. Determine the ROI for a particular security-related project (e.g., the implementation of a patch management capability, a company-wide document shredding service, a Risk Assessment)	30
11	Business Continuity Planning (BCP) – If IT is not ensuring that business functions can continue, and then what is it doing? Contingency Planning – no matter how successful our planning and recover, everything will never go as smoothly as we'd like, what contingency plans do we need to be prepared with.	Develop an ROI for a BCP effort	NIST SP 800-12 (chap. 11), NIST SP 800-34
12	Change Management – undocumented changes to a computing environment can severely hamper business continuity efforts	Research Insurance Policies that cover natural and cyber disasters.	
13	Ethics – decision making skills		Mich Kabay's ethics papers , NIATEC Ethics papers
14	Political Skills – Yes, in order to be effective, the IT department will have to 'play the game'.		
15	Course Project Presentations		