

Cameron School of Business

University of North Carolina Wilmington  
PROPOSAL FOR UNDERGRADUATE CURRICULUM CHANGE

Department or Academic Unit: Information Systems and Operations Management

Type of Proposal: Check **all** that apply and answer the questions below.

New Course (attach syllabus)  Deletion of Course  Degree Requirement  Trial Course

Course Change (Check all that apply):

Prefix/Number  Title  Description  Credit Hours  Contact Hours

Pre/Corequisite  Restrictive Statement  Crosslist  Uncrosslist

Other:

To become effective: Semester: Fall Year: 2009 To be offered:  Fall  Spring  Summer

on Request  Alternate Years

Current course prefix, number and title:

New course prefix, number and title: CIT 324 - Network Security Management

Abbreviated course title (30 spaces maximum): Network Security Mgmt

Type of course:  Lecture  Seminar  Lab  Practicum  Internship  Other

Credit hours: 3 Credit hour change: From: To: Contact hours: 3 Contact hour change: From: To:

Restrictions (If repeatable the number of hours this course may be taken for credit, open only to students within the major, etc.):

Crosslisted with (course prefix and number): Uncrosslist with (course prefix and number):

(To crosslist/uncrosslist courses, a curriculum change form submitted by both departments is required.)

- Yes  No Is this course a renumbering (it replaces an existing course)? If yes, which course?
- Yes  No And should the existing course be deleted? (If yes, a separate curriculum change form requesting this deletion is required.)
- Yes  No Is this course currently approved for basic studies?
- Yes  No Will it be submitted for basic studies approval?
- Yes  No Is this course currently approved for oral competency?
- Yes  No Will it be submitted for oral competency approval?
- Yes  No Is this course currently approved for computer competency?
- Yes  No Will it be submitted for computer competency approval?
- Yes  No Is it required for a major/minor/option in your department? (If yes, please provide in the degree requirement section below the necessary change for degree requirements description in catalogue.)
- Yes  No Is it an elective for a major/minor/option in your department? (If yes, please provide in the degree requirement section below the necessary change for degree requirements description in catalogue.)

Degree requirement as it would appear in the catalogue (Include change to: total hours, new required courses, insertion and deletion of required courses, text, etc.) If additional space is required, prepare on a separate page using the format of the current catalogue and attach to this form.

This course is part of a new degree program in Information Technology. Attached is the Request to Establish a new degree program document that contains all of the degree requirements.

- Yes  No Is it a collateral requirement or elective for a major/minor/option for another department? (If yes, attach documentation listing the departments/programs affected and verifying that the departments were consulted.)
- Yes  No Are present staff and resources adequate to support this proposal? (If no, explain in the justification section how they will be provided.)

University of North Carolina Wilmington  
PROPOSAL FOR UNDERGRADUATE CURRICULUM CHANGE

Course description change as it would appear in the catalogue (Course description change: 50 words or less; include prefix, number, title, credit hours, crosslisting, pre/corequisites, etc.)

CIT 324. Network Security Management (3) Prerequisite: CIT 110 or equivalent. Examination of current standards of due care and best business practices in Information Security. Focus is on evaluation and selection of optimal security posture. Topics include evaluation of security models, risk assessment, threat analysis, organizational technology evaluation, security implementation, disaster recovery planning and security policy formulation and implementation.

Justification for request or degree change:

This course is part of a new degree program in Information Technology. Attached is the Request to Establish a new degree program document.

Yes  No Does this proposal require University Curriculum Committee (UCC) or Faculty Senate approval (refer to <http://www.uncw.edu/faesen/ucc/>)? (If yes, after college/school curriculum committee approval, forward proposal to the UCC and complete and submit the appropriate UCC form(s). If approved, this proposal must be signed by the UCC Chair and Faculty Senate President and forwarded to the Provost.)

Recommended and approved by:

Cem Canel 9-22-08  
Department Chairperson Date

\_\_\_\_\_  
Chair, College or School Curriculum Committee Date

\_\_\_\_\_  
Teacher Education Council (WSE use only) Date

\_\_\_\_\_  
Dean of the College or School Date

\_\_\_\_\_  
\*Chair, University Curriculum Committee Date

\_\_\_\_\_  
\*President, Faculty Senate Date

\_\_\_\_\_  
Provost Date

\*Obtain signatures of the UCC Chair and the Faculty Senate President only if required for this proposal.

Forms not filled out completely or lacking documentation will be returned.

# Network Security Management

## CIT 324

---

### Course Information

**Class Time and Location:** Tuesday-Thursday 11:00am-12:15pm, CIS 1007  
**Instructor:** Ulku Yaylacioglu  
**Office:** CI 2020  
**Office Hours:** MWF 9:30am - 12:30pm  
R 12:30pm - 1:30pm and by appointment  
**Phone:** 962-3901  
**Email:** yaylacioglu@uncw.edu

---

### Course Description

Examination of current standards of due care and best business practices in Information Security. Includes examination of security technologies, methodologies and practices. Focus is on evaluation and selection of optimal security posture. Topics include evaluation of security models, risk assessment, threat analysis, organizational technology evaluation, security implementation, disaster recovery planning and security policy formulation and implementation.

---

### Prerequisites

CIT 110 or equivalent.

---

### Textbook and Materials Required

Principles of Information Security, 2nd Edition by Michael Whitman and Herbert Mattord (3<sup>rd</sup> Edition is also ok)  
Optional: Secrets & Lies: Digital Security in a Networked World by Bruce Schneier  
There will be additional readings assigned throughout the semester.

---

### Handouts

Check SeaPort ([seaport.uncw.edu](http://seaport.uncw.edu)) often. Handouts will be posted after classes. You are responsible for this material irrespective of attendance.

---

### Assessments

Starting from the fourth week of classes, there will be five 15 minutes assessments over the material covered in the previous classes. The material would include the presentations of the instructor, students and guest speakers when applicable.  
**No make-up tests will be offered except on medical grounds.**

---

### Withdrawal Policy

The last day to withdraw without academic penalty is February 26. Ceasing to attend class or oral notice thereof DOES NOT constitute official withdrawal from the course. Students who simply stop attending classes without officially withdrawing usually are assigned failing grades. Students wishing to withdraw after the scheduled change period (add/drop) must obtain and complete a withdrawal form from the Registrar's Office.

---

### Project

---

---

## Requirements

### Topic Paper:

The primary purpose of this assignment is to provide you an opportunity to further develop practical research skills by investigating an information assurance (IA) related topic (hopefully of personal interest). The only apparent constant in the field of information technology and information assurance is change. Business executives are almost constantly barraged with new technical threats and new technical opportunities. Both line managers and IT managers require an ability to filter this information and attempt to discern threats and opportunities that are truly germane to the interests (strategic or otherwise) of the organization. To do this managers need not only an in-depth understanding of their organization's current and proposed operations and strategies, but an ability to recognize and evaluate the potential threats and opportunities arising from changes in the environment. Quite frankly, I don't think anyone knows exactly how to educate an individual to recognize such opportunities. However, I am reasonably certain that having the ability to conduct a reasonable business-type analysis of new capabilities should be helpful.

Accordingly, you are to:

1. select a topic from the following list;
2. write a (2 pages single space – about 1,000 words, Calibri 11 font) executive summary or information paper regarding the topic
3. include an annotated bibliography (with at least four references)
4. give a 10 minutes presentation of your executive summary to class.

Students need to electronically submit Powerpoint slides to instructor at least two days before giving the presentation. The groups will sign-up for presentation days on the first day of class. Projects will be assigned on first-come first-served basis. You are encouraged to start early on the project and touch base with the instructor to ensure you are achieving an appropriate level of detail.

Approved Topics include (if you would like to select an alternative topic please check with me first):

- Spyware
- Control Objectives for Info. and related Technology (COBIT) auditing standards
- Sarbanes-Oxley Act of 2002 (SOX) implications for IT/IA management
- Health Insurance Portability and Accountability Act (HIPAA) implications for IT/IA management
- Identity management
- IA investment analysis
- IA threat analysis
- IA security code checkers
- Secure software development tools
- Trusted computing certification
- Information Technology Infrastructure Library (ITIL) and Security Management

---

**Demo/Hands-On Lab Project:**

Students will pair off into two-member teams to research and prepare a presentation and a demonstration (15-20 minutes) on one of the following security related technologies:

- A software-based open source or commercial network vulnerability scanner (e.g., NESSUS)
- A software-based open source or commercial network analyzer (e.g. Wireshark)
- Active Directory Group Security Policy Management
- A software-based open source or commercial network IDS (e.g., SNORT)
- A software-based open source or commercial network firewall
- An open source or commercial server based IDS or log analysis application
- An open source or commercial server based IDS forensics analysis application (e.g., Sysinternals PStools)
- Students may propose other alternatives which will be subject to instructor approval

**Project deliverables:**

- **Class Presentation:** Electronically submit Powerpoint slides to instructor at least two days before making the presentation. The presentation should as a minimum include: (a) A description of the requirement that the security technology is intended to address; (b) A fairly detailed explanation of how the product functions – emphasizing particularly useful features or capabilities and limitations noted in researching or using the product; (c) A short demonstration of the product configuration and use (using screen shots). The Powerpoint slides should include talking points in the notes section for each slide.
- **Live demonstration:** Depending on the tools and projected time available, each team is to additionally present a demonstration of the product (if you like, you may set up a pre-staged scenario designed to meet a specified set of learning objectives). In the presentation you might include screen shots depicting how you conduct the scan.
- **An annotated bibliography** that identifies sources of material used for the preparation of the presentation and demonstration/lab.

The groups will sign-up for presentation days on the first day of class. Projects will be assigned on first-come first-served basis. If you and a classmate have a particular interest, you need to jump on it. Instructor approval is required for alternative proposals. You are encouraged to start early on the project and touch base with the instructor to ensure you are achieving an appropriate level of detail.

---

**Disabilities**

If you have a disability and need reasonable accommodation in this course, you should inform me of this fact in writing within the first week of class or as soon as possible. If you have not already done so, you must register with the Office of Disability Services in Westside Hall (extension 3746) and obtain a copy of your Accommodation Letter. You should then meet with me to make mutually agreeable arrangements based on the recommendations of the Accommodation Letter.

---

**Grading and**

**Grading Policy** The distribution of the grades will be as follows.

|                                     |     |
|-------------------------------------|-----|
| Assessments and Labs                | 40% |
| Topic paper                         | 25% |
| Demo/Hands-on Lab Project           | 25% |
| Class participation and discussions | 10% |

The grading will be based on the following grading scheme (note +'s and -'s are NOT given in this course).

| <i>Range</i> | <i>Grade</i> |
|--------------|--------------|
| 90 - 100     | A            |
| 80 - 89      | B            |
| 70 - 79      | C            |
| < 70         | F            |

The instructor retains the right to subjectively adjust an individual student's grade in appropriate cases, based upon observed performance.

All turned-in assignments will be neatly typed (word-processed) and printed with letter-quality type. Specific examples will be provided in class. Students failing to present the information completely, neatly and in the prescribed format will receive minimal credit for their work. Students should double check for spelling and grammar before submitting assignments.

Grades can be viewed using Entropy (<http://csbapp.csb.uncw.edu/entropy/>). Please refer to "Registering Entropy" hand-out to create an account.

**Learning Outcomes**

As a result of completing this course, students will be able to:

- Describe threats to information security
- Identify methods, tools and techniques for combating these threats.
- Identify types of attacks and problems that occur when systems are not properly protected.
- Explain integral parts of overall good information security practices.
- Identify and discuss issues related to access control.
- Describe the need for and development of information security policies, and identify guidelines and models for writing policies.
- Define risk management and explain why it is an important component of an information security strategy and practice.
- Describe the types of contingency plan and the steps involved in developing each.
- Identify security issues related to personnel decisions, and qualifications of security personnel.

**Academic**

"Violation of any of the following standards subjects any student to disciplinary

---

**Dishonesty  
Offenses**

action:

**A. PLAGIARISM**

Plagiarism means the appropriation, buying, receiving as a gift, or obtaining by any means another person's work and the unacknowledged submission or incorporation of it in one's own work. It is doubly unethical, since it deprives the true author of his/her rightful credit and then gives that credit to someone to whom it is not due. The following three examples of plagiarism are described by Harold C. Martin and Richard M. Ohmann in their book *The Logic and Rhetoric of Exposition* (1963):

1. **Word-for-Word copying.** Whenever someone else is directly quoted, honesty and courtesy require acknowledgment of the source. The quoted material should be placed in quotation marks and its exact location should be indicated, either in the text of the student's paper or in a footnote.
2. **The mosaic.** To intersperse a few words of one's own here and there while basically copying the work of another is obviously unethical, unless one clearly acknowledges that this is being done. Should there be a valid reason for doing so then quotation marks or a general footnote should be used to show what belongs to the source and what one's own contribution is.
3. **The paraphrase.** Once more the crucial point is acknowledgment. Sometimes one can paraphrase in order to simplify, abbreviate, or improve upon an original, but the reader deserves to know what is being presented to him and whose work it represents. Therefore, acknowledgment of the source is required within the text of the student's paper or by footnote.

**B. BRIBERY**

The offering, giving, receiving or soliciting of any consideration in order to obtain a grade or other treatment not otherwise earned by the student through his/her own academic performance.

**C. CHEATING**

1. Any conduct during a program, course, quiz or examination which involves the unauthorized use of written or oral information, or information obtained by any other means of communication.
  2. The unauthorized buying, selling, trading or theft of any examination, quiz, term paper or project.
  3. The unauthorized use of any electronic or mechanical device during any program, course, quiz, or examination or in connection with laboratory reports or other materials related to academic performance.
  4. The unauthorized use of laboratory reports, term reports, theses, or written materials in whole or in part.
  5. The unauthorized assistance or collaboration on any test, assignment, or project.
  6. The unauthorized use by a student of another student's work or the falsification of any other student's work.
  7. Participating in, or permitting any of the above activities as defined in C 1-6."
- (UNCW Academic Honor Code)
-

**Tentative Schedule**

| <b>Week</b> | <b>Date</b> | <b>Topics</b>   | <b>Assignments</b> |
|-------------|-------------|---|--------------------|
| 1           | 01/10/08    | Course Overview – Intro to Information Assurance                |                    |
| 2           | 01/15/08    | Need for Security   |                    |
|             | 01/17/08    | Need for Security   |                    |
| 3           | 01/22/08    | Legal, Ethical and Professional Issues in Information Security  |                    |
|             | 01/24/08    | Legal, Ethical and Professional Issues in Information Security  |                    |
| 4           | 01/29/08    | Risk Management<br>Topic Paper – Team 1                         | Assessment 1       |
|             | 01/31/08    | Risk Management   |                    |
| 5           | 02/05/08    | Planning for Security<br>Topic Paper – Team 2                   |                    |
|             | 02/07/08    | Planning for Security   |                    |
| 6           | 02/12/08    | Routers as Security Devices<br>Topic Paper – Team 3             |                    |
|             | 02/14/08    | Routers as Security Devices                                     |                    |
| 7           | 02/19/08    | Lab - Router Configuration<br>Topic Paper – Team 4              | Assessment 2       |
|             | 02/21/08    | Lab - Router Configuration                                      |                    |
| 8           | 02/26/08    | <i>BUSINESS WEEK – NO CLASS</i>                                 |                    |
|             | 02/28/08    | <i>Guest Speaker</i>  |                    |
| 9           | 03/04/08    | <i>SPRING BREAK</i>   |                    |
|             | 03/06/08    |   |                    |
| 10          | 03/11/08    | Security Technology: Firewalls and VPNs<br>Topic Paper – Team 5 |                    |
|             | 03/13/08    | Security Technology: Firewalls and VPNs                         |                    |
| 11          | 03/18/08    | Lab – Firewall Configuration                                    | Assessment 3       |
|             | 03/20/08    | <i>STATE HOLIDAY</i>  |                    |
| 12          | 03/25/08    | Security Technology: Intrusion Detection and Access Control     |                    |
|             | 03/27/08    | Security Technology: Intrusion Detection and Access Control     |                    |
| 13          | 04/01/08    | Cryptography<br>Project – Team 1                                |                    |
|             | 04/03/08    | Cryptography  |                    |
| 14          | 04/08/08    | Physical Security<br>Project – Team 2                           |                    |
|             | 04/10/08    | Physical Security   |                    |
| 15          | 04/15/08    | Implementing Information Security<br>Project – Team 3           | Assessment 4       |
|             | 04/17/08    | Implementing Information Security                               |                    |
| 16          | 04/22/08    | Security and Personnel<br>Project – Team 4                      |                    |
|             | 04/24/08    | Information Security Maintenance<br>Project – Team 5            |                    |
| 18          | 05/06/07    |   | Assessment 5       |