Center for Professional Development
ILLINOIS INSTITUTE OF TECHNOLOGY www.iit.edu

8.28.05

Proposal for the Master of Information Security Technologies & Management Degree Program

Background

The need for qualified information security personnel with knowledge covering technology, business, management and law has grown enormously with the emergence of hackers, cyber-crime and even cyber-terrorism as major threats in the twenty-first century. The Center for Professional Development at Illinois Institute of Technology is uniquely positioned to provide a quality educational program to equip students for the role of Chief Information Security Officer (CISO) at the enterprise level through a Master of Information Security Technologies & Management degree. Building on a core of existing courses from the Information Technology &Management (ITM) program and providing at least three new courses, the program would also expand options for students in the Master of Information Technology & Management degree.

Information Technology & Management Degree Programs,
Center for Professional Development
201 E. Loop Rd.
Wheaton, Illinois 60187

630.682.6000
630.682.6010 Fax

www.cpd.iit.edu

Proposal

The Master of Information Security Technologies & Management (MISTM) degree would be a thirty-credit professional masters program. Courses would primarily be drawn from the Information Technology and Management Program (ITM) program, but courses could come from other academic units within the university as well. The intent is to present a balanced program with equal emphasis on all aspects of information security—both technical and managerial—at an enterprise level.

Admission

Applicants for admission must have earned a four-year bachelors degree from an accredited institution with a minimum cumulative undergraduate GPA of 3.0/4.0. Applicants should have an undergraduate degree in a computer-related area, and additionally must have experience as information technology or computer science professionals and should be prepared to provide a work history and references to confirm this experience. International applicants are required to submit a GRE score with a minimum score of 1200 (combined score for tests taken prior to Oct. 1, 2002) or 900 (quantitative + verbal) and 2.5 (analytical writing) (for tests taken on or after Oct. 1, 2002) and may be required to submit a TOEFL score (see page 26). Admission as a non-degree student follows the university policy set forth in the bulletin.

RET:ret

Prerequisites
Information Security Technologies & Management students who are deficient in knowledge or experience in certain areas of information technology will be required to demonstrate proficiency in undergraduate courses that are prerequisites for this graduate program. Proficiency may be demonstrated by taking and passing a written exam or taking and passing, with a grade of "B" or better, the prerequisite courses at IIT. Current prerequisites for the Master of Information Security Technologies & Management include an ability to program at a basic level using a contemporary object-oriented programming language
(ITM 311 or ITM 312 or equivalent coursework, certification or experience) and knowledge and experience in computer networking (ITM 440 or ITM 540 or equivalent coursework, certification or experience; MISTM students may take ITM 540 for credit as a degree elective).

Degree Requirements
30 credit hours
(Courses may be selected from 400-and 500-level courses: a minimum of 18 credit hours must be at the 500-level or higher.)
GPA of 3.0/4.0 or better

Students are required to complete six hours of core courses and another twelve hours selected from Information Security Technologies & Management electives. The final twelve hours of electives may be selected from any courses in the Information Technology & Management program or (with the advisor's consent) other IIT academic units, and should be additional MISTM courses, prerequisites for MISTM courses, or courses that complement specific areas of security focus selected by the student.

Curriculum

Required Core Courses

- ITM 548 System and Network Security
- ITM 578 Information System Security Management

Four electives selected from the following courses:

- ITM 528 Database Security
- ITM 538 Computer & Network Forensics
- ITM 543 Digital Voice Communication Security [new course]
- ITM 549 System and Network Security: Projects & Advanced Methods
- ITM 558 Operating System Security
- ITM 574 Strategic Information Technology Management
- ITM 585 Legal and Ethical Issues in Information Technology
- ITM 588 Disaster Recovery & Business Continuity [new course]
- ITM 589 Information Security Risk Assessment and Analysis [new course]

Four electives selected from existing Information Technology & Management courses and/or other IIT courses

- These courses could be additional MISTM courses, prerequisites for MISTM courses, or courses that complement specific areas of security focus selected by the student

Target Market
This would be an ideal master's program for information technology professionals who are in or desire to enter the information security field. This would be an outstanding second advanced degree for those who already hold an MBA.

Course Descriptions

ITM 528 Database Security
Students will engage in an in-depth examination of topics in data security including security considerations in applications & systems development, encryption methods, cryptography law and security architecture & models. Prerequisite: ITM 421 (3-0-3)

ITM 538 Computer & Network Forensics (draft)
This course will address methods to properly conduct a computer and/or network forensics investigation including digital evidence collection and evaluation and legal issues involved in network forensics. Technical issues in acquiring court-admissible chains-of-evidence using various forensic tools that reconstruct criminally liable actions at the physical and logical levels are also addressed. Prerequisite: ITM 548 (2-2-3)

ITM 543 Digital Voice Communications Security (draft)
Addresses security issues inherent in Voice over IP and other digital voice transport implementations, including hands-on laboratory experience in the technical management of security for digital voice. Security protocols, encryption, identity and authentication will all be covered. Students will complete a team project. Prerequisites: ITM 546, ITM 548 (2-2-3)

ITM 548 System and Network Security
Prepares students for a role as a network security administrator and analyst. Topics include viruses, worms, other attack mechanisms, vulnerabilities and countermeasures, network security protocols, encryption, identity and authentication, scanning, firewalls, security tools, and organizations addressing security. A component of this course is a self-contained team project that, if the student wishes, can be extended into a fully operational security system in a follow-on course. Prerequisite: ITM 540 (2-2-3)

ITM 549 System and Network Security: Projects & Advanced Methods
Prepares students for a role as a network security analyst and developer and give the student experience in developing a production security system. Topics may include computer and network forensics, advances in cryptography and security protocols and systems; operating system security, analysis of recent security attacks, vulnerability and intrusion detection, incident analysis, and the design and development of secure networks. This course includes a significant real world team project the results in an fully operational security system. Students should have previous experience with object-oriented and/or scripting languages. Prerequisite: ITM 548 (2-2-3) (C)

ITM 558 Operating System Security (draft)
This course will address theoretical concepts of operating system security, security architectures of current operating systems, and details of security implementation using best practices to configure operating systems to industry security standards. Server configuration, system-level firewalls, file system security, logging, anti-virus and

anti-spyware measures and other operating system security strategies will be examined. Prerequisite: ITM 301 or ITM 302 (2-2-3)

ITM 574 Strategic Information Technology Management
This course defines information technology management strategies, explores the possible information technology strategies of an organization, and provides conceptual frameworks for the development and evaluation of information technology management strategies. It also examines concepts of strategic information technology systems, approaches for analyzing strategic applications, and systems planning as it relates to information technology management strategy and the interface with organizational strategies. (3-0-3)

ITM 578 Information System Security Management
In-depth examination of topics in the management of information technology security including access control systems & methodology, business continuity & disaster recovery planning, legal issues in information system security, ethics, computer operations security, physical security and security architecture & models using current standards and models. Students working in teams will conduct an information security program audit for a real-world organization such as a business or a government body or agency.(3-0-3)

ITM 585 Legal and Ethical Issues in Information Technology
Current legal issues in information technology are addressed including elements of contracting, payment systems and digital signatures, privacy concerns, intellectual property, business torts and criminal liability including hacking, computer trespass and fraud. Examination of ethical issues including privacy, system abuse, and ethical practices in information technology equip students to make sound ethical choices and resolve legal and moral issues that arise in information technology. (3-0-3)

ITM 588 Disaster Recover and Business Continuity (draft)
Students learn to design and manage key business information security functions including incident response plans and incident response teams; disaster recovery plans; and business continuity plans. Reporting, response planning and budgeting are all addressed. Students working in teams will prepare an incident response, disaster recovery, or business continuity plan for a real-world organization such as a business or a government body or agency. Prerequisite: ITM 578 (3-0-3)

ITM 589 Information Security Risk Assessment and Analysis (draft)
Students will learn the details of risk management in information security. Risk assessment involves estimating harm to business likely to result from a security failure and the likelihood of such a failure. Risk analysis is the process of indentifying an organization's information resources, existing controls, security risks, and vulnerabilities; determining their magnitude; and indentifying areas needing safeguards as well as establishing potential costs. Students working in teams will conduct a risk assessment or risk analysis for a real-world organization such as a business or a government body or agency. Prerequisite: ITM 578 (3-0-3)