THOMPSON RIVERS UNIVERSITY

Course Outline

Department of Management
School of Business and Economics

MIST 4620-3
Information Security Management for Business (3,0,0)

Calendar Description

Students develop a general understanding of information technology security. Dependency on computer technology and the Internet has grown to a level where all organizations must devote considerable resources to managing threats to the security of their mobile, desktop and networked computer systems. Topics include introduction to information security; basic need for security; legal, ethical, and professional issues; risk management; information security planning; security technologies such as firewalls and VPN's; detection and prevention security technologies; cryptography; and implementation and maintenance of information security.

Educational Objectives/Outcomes

Upon completing this course, students will be able to:

1. Explain the basic concepts of information security.
2. Describe the threats to the security of computer systems.
3. Summarize legal requirements of data protection and laws regulating the use of data in business.
4. Identify risks and develop a risk management plan.
5. Outline a complete information security plan.
6. Understand methods of detecting threats and protecting computer networks from external attacks.
7. Illustrate the use of different encryption techniques.
8. Implement a small information security plan.
9. Manage daily information security tasks.

Prerequisites

CMNS 1290; MIST 2610

Co-requisites

None

Texts/Materials

Whitman, Michael, Mattord, Herbert, Principles of Information Security, 4th Edition, Course Technology Cengage Learning.

Woody, Aaron, Enterprise Security: A Data-Centric Approach to Securing the Enterprise, 1st Edition, Packt Publishing.

Rhodes-Ousley, Mark, Information Security: The Complete Reference, 2nd Edition, McGraw Hill.

Student Evaluation

Participation	0%-10%
Tests/quizzes	20%-30%
Case studies/projects/assignments	20%-30%
Final exam	30%-45%

Students must pass the final exam to pass the course.

Course Topics

1. Introduction to Information Security
   - The History of Information Security
   - Key Information Security Concepts
   - Components of Information Systems
   - Information Security Implementation

2. Basic Need for Security
   - Protecting Data
   - Mobile Computing
   - Cloud Computing
   - Threats
     - Compromises to Intellectual Property
     - Deliberate Software Attacks
     - Human Error and Failure
     - Information Extortion
     - Inadequate Organizational Policy or Planning
     - Physical Security (Trespassing, Sabotage, Theft)
     - Hardware and Software Failures
   - Attacks
     - Malicious Code
     - Hoaxes
     - Back Doors
     - Password Cracks
     - Denial-of-Service
     - Spoofing
     - Spam
     - Mail Bombing
     - Sniffers
     - Social Engineering

3. Legal, Ethical, and Professional Issues

- Organizational Liability
- Relevant Canadian Laws and Regulations (financial reporting, local regulations)
- Privacy
- Copyright Laws
- International Laws
- Ethics and Information Security

4. Risk Management
   - Risk Identification
   - Asset Identification and Inventory
   - Classifying and Prioritizing Information Assets
   - Identifying and Prioritizing Threats
   - Vulnerability Identification
   - Risk Determination and Assessment
   - Risk Control Strategies **(**Defend**,** Transfer**,** Mitigate**,** Accept**,** Terminate)
   - Best Practices in Risk Control Practices

5. Information Security Planning
   - Information Security Policy, Standards, and Practices
     - The ISO 2700
     - NIST Security Models
     - IETF Security Architecture
     - Design of Security Architecture
   - Security Education, Training, and Awareness Program
   - Continuity Strategies
     - Business Impact Analysis
     - Incident Response Planning
     - Disaster Recovery Planning
     - Business Continuity Planning

6. Security Technologies: Firewalls and VPN's
   - Access Control **(**Identification**,** Authentication**,** Authorization**,** Accountability)
   - Firewalls
   - Configuring and Managing Firewalls
   - Securing Remote Connections

7. Detection and Prevention Security Technologies
   - Intrusion Detection and Preventions Systems (IDPS)
   - Scanning and Analysis Tools
   - Firewall Analysis Tools
   - Wireless Security Tools
   - Biometric Access Controls

8. Cryptography
   - Foundation of Cryptology
   - Cipher Methods
   - Cryptographic Algorithms
   - Cryptographic Tools

- Protocols of Secure Communications
- Attacks on Cryptosystems

9. Implementing Information Security
   - Technical Implementation Issues
   - Security Certification and Accreditation
   - Staffing the Information Security Functions
   - Credentials of Information Security Professionals

10. Information Security Maintenance
   - Monitoring the External Environment
   - Monitoring the Internal Environment
   - Digital Forensics
   - Planning and Risk Assessment
   - Vulnerability Assessment and Remediation

Methods for Prior Learning Assessment and Recognition

As per TRU policy

Attendance Requirements – Include if different from TRU Policy

As per TRU policy

Special Course Activities – Optional

Use of Technology – Optional