RYERSON UNIVERSITY

Ted Rogers School of Information Technology Management
and G. Raymond Chang School of Continuing Education

COURSE OF STUDY
2017-2018

(C)ITM 820 – Information Systems Security and Privacy

1.0 PREREQUISITE

The prerequisite for this course is ITM 301. Students who do not have the prerequisite will be dropped from the course.

2.0 INSTRUCTOR INFORMATION

- Name:
- Office Phone Number:
- E-mail address:
- Faculty/course web site(s): https://my.ryerson.ca
- Office Location & Consultation hours:
    - Your instructor is available for personal consultation during scheduled consultation hours which are posted on their office door or on the course shell in D2L Brightspace. However, you are advised to make an appointment by e-mail or by telephone before coming to ensure that the professor is not unavoidably absent.
- E-mail Usage & Limits:

Students are expected to monitor and retrieve messages and information issued to them by the University via Ryerson online systems on a frequent and consistent basis. ***Ryerson requires that any official or formal electronic communications from students be sent from their official Ryerson E-mail account.*** As such emails from other addresses may not be responded to.

3.0 CALENDAR COURSE DESCRIPTION

This course considers the technical, operational, and managerial issues of computer and network security in an operational environment. Industry best-practices relating to computer security including schemes for breaking security, and techniques for detecting and preventing security violations are the core focus of this course. This course will also explore the principles of data privacy, threats to privacy, international and national policy, particularly related to privacy-enhancing technologies as they apply to the management of information systems and e-Business.

4.0 COURSE OVERVIEW

This course provides the opportunity for the student to explore computer security and network security in an operational environment. Current industry best practices relating to computer security including schemes for breaking security, and techniques for detecting and preventing security violations are core focus of this course. Emphasis will be on the development of appropriate safeguards, the study of different types of security systems, and the development of appropriate security for the perceived risk. Each student will explore various aspects of computer security through assignments, software deployment, selected readings and a group research project.

5.0 COURSE OBJECTIVES

This course provides students with a detailed review of the industry-accepted methods for securing computer applications and computer networks. The course will provide an awareness of the risks and threats to computer operations and communications and an overview of the different types of security techniques. The course will address issues and challenges associated with implementing the appropriate level of security to meet the needs of the organization.

Upon completion of the course, students should be able to:

1. Explain the fundamental principles of Information Technology Security and Privacy, and Data Protection.
2. Explain the concepts of threat, evaluation of assets, information assets, physical, operational, and information security, and how they are related.
3. Describe the need for the careful design of a secure organizational information infrastructure
4. Describe risk analysis and risk management in the context of business.
5. Describe both technical and administrative mitigation approaches.
6. Explain the need for a comprehensive security model and its implications for the security manager.
7. Demonstrate knowledge of security technologies.
8. Demonstrate knowledge of basic cryptography, its implementation considerations, and key management.
9. Demonstrate knowledge of designing and guiding the development of an organization’s security policy.
10. Demonstrate knowledge of determining appropriate strategies to assure confidentiality, integrity, and availability of information.
11. Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls.
12. Describe privacy issues associated with storing and distributing digital data.
13. Explain Privacy-by-Design (PbD) framework.
14. Explain security issues associated with the emergent cloud computing technology.

6.0 EVALUATION

The grade for this course is composed of the mark received for each of the following components:

Evaluation Component	Percentage of the Final Grade
Four Assignments (5% each)	20%
Group Project	10%
Midterm Examination	30%
Final Examination	40%
Total	**100%**

NOTE: Students must achieve a course grade of at least 50% to pass this course.

Citation Format for Essays and Term Papers
All essay assignments, term paper and other written works must adhere with APA citation format. Technical errors (spelling, punctuation, proofing, grammar, format, and citations) and/or inappropriate levels of language or composition will result in marks being deducted. You are encouraged to obtain assistance from the Writing Centre (www.ryerson.ca/writingcentre) for help with your written communications as needed.

You can find APA guidelines and academic referencing from the following online resources:

a) Ryerson Writing Support Web site:
http://www.ryerson.ca/content/dam/studentlearningsupport/resources/citation-conventions/APA%20Basic%20Style%20Guide.pdf

b) Ryerson Library for APA style guide: https://library.ryerson.ca/guides/style/

7.0 POSTING OF GRADES

- All grades, on assignments or tests must be posted or made available to students through the return of their work. Grades on final exams must be posted. However, as there may be other consideration in the determination of final grades, students will receive their official final grade in the course only from the Registrar. Final official course grades may not be posted or disclosed anywhere by an instructor.
- Posting of grades on the Course Management System (D2L Brightspace) is preferred. If grades are posted in hard copy they must be posted numerically sorted by student identification number after at least the **first four digits** have been removed. Instructors must inform students in all course management documentation of the method to be used in the posting of grades. Students who wish not to have their grades posted must inform the instructor in writing.
- Some graded work will be returned to students prior to the last date to drop a course without academic penalty.

8.0 TOPICS – SEQUENCE & SCHEDULE

Session	Topic	Learning Outcomes	Readings	Activities & Due Dates
1	Security Concepts: Introduction, Framework	● Explain what assets we need to protect. ● Explain how those assets are threatened. ● Explain the best options to counter those threats. ● Explain confidentiality, integrity and availability triad	Ch. 1 Lecture Notes	
2	Cryptographic Tools: Symmetric Encryption, Public Key Encryption, Hash Functions, Digital Signatures	● Describe various types of algorithms and their applications ● Explain the basics of encryption ● Describe modern cryptography methods ● Describe message authentication methods	Ch. 2 Lecture Notes	
3	User Authentication: Password, Token and Biometric Authentication; Access Control: Access Control and Access Management	● Describe the four general means of authenticating a user's identity ● Explain passwords authentication methods ● Describe token-based user authentication ● Explain how access controls & user authentication ● Distinguish among subjects, objects, and access rights	Ch. 3 & 4	**Assignment 1**
4	Database and Cloud Security: Database Access Control, SQL Injection Attacks Data Protection in the Cloud	● Discuss the unique need for database security ● Describe SQL injection attacks ● Compare different approaches of database security ● Discuss key concepts of cloud security	Ch. 5 Lecture Notes	
5	Malicious Software: Viruses, Worms, SPAM, Trojans, Bots, Phishing, Spyware, Rootkits	● Describe three broad malware uses to propagate ● Discuss the basic operations of viruses, worms, Trojan horses, and logic bombs ● Discuss the different threats posed by bots, spams, spyware, and rootkits ● Discuss the backdoor vulnerabilities of systems	Ch. 6 Lecture Notes	**Assignment 2**
6	Security Attacks: Denial of Service Attacks, Man-in-the-middle Attack, Spoofing, Sniffing	● Explain the basic concepts of DoS & DDoS attacks ● Describe flooding attacks ● Explain man-in-the-middle attacks ● Explain spoofing and sniffing, and their negative impacts on business	Ch. 7 Lecture Notes	**Intro. to Group Project**
7	**Midterm Examination** Firewall, Intrusion Detection and Prevention Systems	● Explain snort architecture ● Explain the purpose of honeypots ● Describe different types of honeypots and sandboxes ● Explain the role of firewalls,	Ch. 8 & 9 Lecture Notes	

		proxies, and NAT in a network		
8	Operating System Security: System Security, Linux/UNIX and Windows Security Trusted Computing and Multilevel Security	● Explain the features of Windows and Linux\Unix security ● Discuss virtualization and hypervisor management ● Explain multilevel security ● Discuss hardware approaches to trusted computing model ● Explain the concept of security assurance ● Explain C2 security evaluations	Ch. 12 & 13	**Assignment 3**
9	Wireless Network Security Privacy Enhancing Technologies	● Explain components of 802.11 standards and WLAN ● Explain WEP and WPA authentication methods ● Describe advanced features of 802.11i technology ● Explain security vs. privacy ●Describe Privacy by Design (PbD) framework ● Explain the concept of privacy acts such as EU directives, PIPEDA, and ISO standards	Ch. 24 Lecture Notes	
10	IT Security Management and Risk Assessment Security Controls, Plans and Procedure	● Explain ISO IT security standards ● Explain the process involved in IT security management ● Discuss organizational IT security policy ● Discuss IT security plans ● Identify security threats and security risk assessments	Ch. 14 & 15	**Assignment 4**
11	Symmetric Encryption and Message Confidentiality	● Describe the general model for the symmetric encryption process. ● Describe block encryption algorithms: DES, 3DES, and AES. ● Describe stream cipher RC4. ● Examine the application of symmetric algorithms to achieve confidentiality.	Ch. 20 Lecture Notes	
12	Security Auditing, Legal and Ethical Aspects Physical and Infrastructure Security: Prevention, Mitigation, Recovery	● Describe the process of security compliance, audits, and trails ● Discuss measures for physical disaster and recovery plans ● Discuss physical and logical security integration ● Describe benefits of security awareness, training, and education	Ch. 16, 18 & 19 Lecture Notes	**Group Project**

9.0 TEACHING METHODS

This course will incorporate the following teaching and learning methods:
● Regular lectures, prescribed weekly readings, problem based assignments, group project work, and case study discussions are the main teaching activities that occur in this course.
● Since a major component of this course is problem-based learning the four individual assignments provide the students practice and progressive skill-building that they can apply in the group based project.

● The group project work allows the students to apply the analytical techniques that were introduced in class and practiced in the problem sets. In addition, by working in small teams the students develop group interaction and individual and group presentation skills.
● The instructor will establish an active learning environment by engaging the students in a Socratic exchange of relevant questions and ideas. Students should expect a frequent and substantive interaction between the instructor and students and among students in every class.
● Those students that actively participate in the learning process will gradually assume ownership of the knowledge contained in the course materials. In addition to ownership of the course content, the students will master a set of skills that they can use to develop communications networks.

10.0 TEXTS & OTHER READING MATERIALS

Title: Computer Security: Principles and Practice, 3rd Edition
Author: William Stallings and Lawrie Brown
Publisher: Prentice Hall (Pearson)
ISBN: 978-0133773927

Suggested/Recommended Textbook
Title: Cloud Computing, Automating the Virtualized Data Center
Authors: Venkata Josyula, Malcom Orr & Greg Page
Publisher: Cisco Press
ISBN: 978- 1285448367

Title: Principles of Information Security (5th Edition)
Authors: Michael E. Whitman, Herbert J. Mattord
Publisher: Course Technology
ISBN: 978-1587204340

11.0 VARIATIONS WITHIN A COURSE

All sections of a course (Day and CE sections) will follow the same course outline and will use the same course delivery methods, methods of evaluation, and grading schemes. Any deviations will be posted on D2L Brightspace once approved by the course coordinator.

12.0 OTHER COURSE, DEPARTMENTAL, AND UNIVERSITY POLICIES

- For more information regarding course management and departmental policies, please consult the **'Appendix of the Course of Study'** which is posted on the Ted Rogers School of Information Technology Management website, http://www.ryerson.ca/content/dam/itm/documents/cos/Appendix.pdf. This appendix covers the following topics:
  - **12..1** Attendance & Class Participation
  - **12..2** Email Usage
  - **12..3** Request for Academic Consideration
    - **12..3.1** Ryerson Health Certificate
    - **12..3.2** Academic Accommodation for Students with Disabilities
    - **12..3.3** Religious, Aboriginal or Spiritual Observance
    - **12..3.4** Re-grading and Recalculation
  - **12..4** Examinations & Tests
    - **12..4.1** Period of Prohibition from Testing

12..4.2 Make-Up of Mid-Term Tests, Assignments and Other Assessments During the Semester
12..4.3 Make –Up of Final Exams
12..4.4 Missing a Make-Up
12..5 Late Assignments
12..6 Standard of Written Work
12..7 Academic Grading Policy
12..8 Academic Integrity
12..8.1 Turnitin.com
12..9 Student Rights