TED ROGERS SCHOOL
Information Technology Management

Ryerson University
The Chang School of Continuing Education

RYERSON UNIVERSITY

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

(C)ITM 820 – Information Systems Security and Privacy

COURSE OUTLINE FOR 2020-2021

1.0 PREREQUISITE(S)

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 virtual consultation during scheduled consultation hours. Information on the consultation format is provided in the D2L course shell. If you wish to make an appointment, kindly do so via email to ensure the professor is available.
- E-mail Usage & Limits:

Students are expected to monitor and retrieve messages and information sent through D2L and Ryerson email on a frequent and consistent basis. In accordance with the policy on Ryerson student email accounts (Policy 157), Ryerson requires that any electronic communication by students to Ryerson faculty or staff be sent from their official Ryerson email account. Messages from other accounts may be disregarded.

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 OBJECTIVES AND LEARNING OUTCOMES

Learning outcomes describe what students are expected to have learned or achieved; as a result, they usually describe what students will be capable of doing, or what evidence will be provided to substantiate learning.

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.

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.

5.0 TEXTS & OTHER READING MATERIALS

Title: Computer Security: Principles and Practice, 4th Edition
Author: William Stallings and Lawrie Brown
Publisher: Pearson
ISBN: 978-0134794105

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 (6th Edition)
Authors: Michael E. Whitman, Herbert J. Mattord
Publisher: Course Technology
ISBN: 978-1337102063

6.0 TEACHING METHODS

In Fall 2020 this course will be taught will be taught remotely in virtual classrooms. Instruction will take place at scheduled hours, following the approach outlined in D2L Brightspace. You will not be required to attend the Ryerson University campus to complete this course.

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.

7.0 EVALUATION, ASSESSMENT AND FEEDBACK

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.

- ❖ At least **20%** of student's grade based on individual work will be returned to students prior to the last date to drop a course in good academic standing .

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:

Student Learning Support > Online Resources > Writing Support Resources

- APA Basic Style Guide

Ryerson Library Citations and Style Guides

- APA Style

8.0 PLAGIARISM DETECTION

Turnitin (if used in this course)

Turnitin.com is a plagiarism prevention and detection service to which Ryerson subscribes. It is a tool to assist instructors in determining the similarity between students' work and the work of other students who have submitted papers to the site (at any university), internet sources, and a wide range of books, journals and other publications. While it does not contain all possible sources, it gives instructors some assurance that students' work is their own. No decisions are made by the service; it generates an "originality report," which instructors must evaluate to judge if something is plagiarized.

Students agree by taking this course that their written work will be subject to submission for textual similarity review to Turnitin.com. Instructors can opt to have student's papers included in the Turnitin.com database or not. Use of the Turnitin.com service is subject to the terms-of-use agreement posted on the Turnitin.com website. Students who do not want their work submitted to this plagiarism detection service must, by the end of the second week of class, consult with their instructor to make alternate arrangements.

Even when an instructor has not indicated that a plagiarism detection service will be used, or when a student has opted out of the plagiarism detection service, if the instructor has reason to suspect that an individual piece of work has been plagiarized, the instructor is permitted to submit that work in a non-identifying way to any plagiarism detection service.

Virtual Proctoring (if used in this course)

Online exam(s) within this course use a virtual proctoring system. Please note that your completion of the exam will be recorded via the virtual platform and subsequently reviewed by your instructor. The virtual proctoring system provides the instructor with a recording that only includes video where possible indications of suspicious behaviour are identified. Recordings will be held for a limited period of time in order to ensure academic integrity is maintained.

Access to a computer that can support remote recording is your responsibility as a student. The computer should have the latest operating system, at a minimum Windows (10, 8, 7) or Mac (OS X 10.10 or higher) and web browser Google Chrome or Mozilla Firefox. You will need to ensure that you can complete the exam using a reliable computer with a webcam and microphone available, as well as a high-speed internet connection. Please note that you will be required to show your Ryerson OneCard prior to beginning to write the exam. In cases where you do not have a Ryerson OneCard, government issued ID is permitted.

Information will be provided prior to the exam date by your instructor who may provide an opportunity to test your set-up or provide additional information about online proctoring. Since videos of you and your environment will be recorded while writing the exam, please consider preparing the background (room / walls) so that personal details are not visible, or move to a room that you are comfortable showing on camera.

9.0 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 the concept of	Ch. 1 Lecture Notes	

		security assurance and evaluation		
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 - access controls & user authentication ● Distinguish among subjects, objects, and access rights	Ch. 3 & 4	**Assignment 1**
4	Database and security attacks: Database Access Control, SQL Injection Attacks Data protection in Cloud	● Discuss the unique need for database security ● Describe SQL injection attacks ● Compare different	Ch. 5 Lecture Notes	

		approaches of database security ● Discuss key concepts of cloud security		
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	Ch. 8 & 9 Lecture Notes	

		honeypots and sandboxes ● Explain the role of firewalls, proxies, and NAT in a network		
8	Operating System Security: System Security, Linux/UNIX and Windows Security Privacy Enhancing Technologies	● Explain the features of Windows and Linux\Unix security ● Discuss virtualization and hypervisor management ● 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. 12	**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	Ch. 19 & 24 Lecture Notes	
10	IT Security Management and Risk Assessment Security Controls, Plans and Procedure	● Explain ISO IT security standards ● Discuss organizational IT security policy	Ch. 14, 15	**Assignment 4**

		● Discuss IT security plans ● Identify security threats and security risk assessments		
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 Lecture Notes	**Group Project**

10.0 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.

11.0 OTHER COURSE, DEPARTMENTAL, AND UNIVERSITY POLICIES

For more information regarding course management and departmental policies, please consult the Course Outline Appendix which is posted on the Ted Rogers School of Information Technology Management website.

NOTE: Students must adhere to all relevant university policies found in their online course shell in D2L and /or on the following URL: senate-course-outline-policies.

The appendix covers the following topics:

Attendance & Class Participation

Email Account

Request for Academic Consideration

Examinations & Tests

Late Assignments

Standard of Written Work

Academic Grading Policy

Academic Integrity

Student Rights

Important Resources Available at Ryerson

- Academic Accommodation Support: Ryerson University acknowledges that students have diverse learning styles and a variety of academic needs. If you have a diagnosed disability that impacts your academic experience, connect with Academic Accommodation Support (AAS). Visit the AAS website or contact aasadmin@ryerson.ca for more information. Note: All communication with AAS is voluntary and confidential, and will not appear on your transcript.

- The Library provides research workshops and individual assistance. If the University is open, there is a Research Help desk on the second floor of the library, or go to Workshops.

- Student Learning Support offers group-based and individual help with writing, math, study skills, and transition support, as well as resources and checklists to support students as online learners.

- You can submit an Academic Consideration Request when an extenuating circumstance has occurred that has significantly impacted your ability to fulfill an academic requirement.

- Ryerson COVID-19 Information and Updates for Students summarizes the variety of resources available to students during the pandemic.

- Familiarize yourself with the tools you will need to use for remote learning. The Continuity of Learning Guide for students includes guides to completing quizzes or exams in D2L or Respondus, using D2L Brightspace, joining online meetings or lectures, and collaborating with the Google Suite.