TELFER

VOTRE LIEN AVEC CE QUI COMPTE — CONNECTS YOU TO WHAT MATTERS

EBC6170: Internet Security

Course Outline – Fall 2018

Professor: Dr. Umar Ruhi
Email: umar.ruhi@uottawa.ca
Office: DMS 6148
Tel: 613-562-5800 X. 1990
Office Hours: Book Online at http://umar.biz/contact

1. Class Convention:

Wednesdays from 4:00 p.m. to 7:00 p.m. in VNR 3075

2. Course Overview and Objectives:

In this day and age, not only are information and communication technologies (ICTs) inextricably linked with multiple aspects of our everyday lives, their use leads to a multitude of concerns surrounding computer, information, and physical security. Cyber security mechanisms and practices always influence and often predominate the design and implementation of many internet based technologies and also affect the feasibility of E-Business ventures. Ultimately, it remains a challenge to design a system that can efficiently balance risk with service. *This course presents a foundation level view of the technical, managerial and human behavioral factors that are important for the effective implementation and institutionalization of security technologies, mechanisms, standards and practices*. The objective of this course is to build an expansive understanding of technical, managerial, ethical, and legal issues related to the security of information systems with more specific emphasis on E-Business technologies. Toward this, the course covers a variety of topics including user, data and network security principles, information security strategies, risk assessment frameworks, operations security, access control systems, network security architectures, encryption and public key infrastructures, international security measurement standards, and regulatory compliance.

3. Course Materials:

OWASP & NIST Publications: This course will largely utilize the standards and practices recommended by OWASP (Open Web Application Security Project) and NIST's (the National Institute of Standards & Technology) Computer Security Division. Specifically, the course will draw upon content from sections the following documents:

- OWASP Application Security Guide for CISOs (V 1.0, November 2013): https://www.owasp.org/images/d/d6/Owasp-ciso-guide.pdf
- SP 800-100 (Information Security Handbook: A Guide for Managers) accessible at: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

Electronic Articles: The discussion in this course will also draw upon contemporary body of knowledge from academic journals, practitioner periodicals, and industry case studies. Readings for each discussion session will be assigned from various electronic sources that are accessible through the library portal of the University of Ottawa and/or the course website.

Online Repository: Brightspace D2L will be utilized in this course as the content, communication and collaboration medium linking the instructor and students. Additional details will be provided during the second week of classes. The website will act as a front-end to the document repository which will be used for storing lecture notes, handouts, and other electronic supplements. It is your responsibility to check the course website regularly for any announcements and/or updates. If you experience any technical difficulties with the course website, please email me at umar.ruhi@uottawa.ca for help.

4. Tentative Course Schedule:

The topics in this course can generally be categorized along the themes of: i) ***Security Management Practices*** ii) ***Security Systems Architecture*** and iii) ***Security Systems Infrastructure***. The following tentative class schedule outlines the seminar discussion themes for each lecture session.

Date	Discussion Themes	Milestones & Deliverables
Oct. 31	▪ **Course Overview** ▪ **Introduction to Information Systems Security** ▪ **IS Security Frame of Reference: Technical, Formal and Informal Dimensions** ▪ **Security Planning Process and Principles**	
Nov. 07	▪ **IS Security Standards & Frameworks** ▪ **PCI Security Standards** ▪ **Basics of Availability & Reliability** ▪ **Authentication, Authorization & Access Control Mechanisms**	▪ **Workgroup Team Roster via Email Memo (Nov. 5th)** ▪ **Case Selection Online (Nov. 9th)**
Nov. 14	▪ **Authentication Mechanisms (contd.)** ▪ **Solution Provider Case Study** ▪ **Assignment Overview & Workshop/Tutorial (with TA)**	▪ **Assignment Workshop/Tutorial**
Nov. 21	▪ **Security Risk Analysis Heuristics & Frameworks**	
Nov. 28	▪ **Security Risk Analysis Heuristics & Frameworks (contd.)** ▪ **Security & Risk Management in Cloud Computing** ▪ **Cryptography, Encryption & Public Key Infrastructure (PKI)**	▪ **IS Security Risk Management Mini-Case Solution & Discussion**
Dec. 05 & TBD	▪ **Cryptography, Encryption & PKI (contd.)** ▪ **Case Discussion Forum**	▪ **Case Discussion Forum I (Teams TBD)**
	▪ **Course Wrap-Up** ▪ **Case Discussion Forum**	▪ **Case Discussion Forum II (Teams TBD)** ▪ **Technology Tool Pilot Assignment (Dec. 7th)**
	▪ **Take-Home Final Exam**	▪ **Take-Home Final Exam (Posted: Dec. 10th ; Due: Dec. 18th)**

Notes:

i) The course schedule may be modified as necessary to meet the course learning objectives. Any such changes will be announced, in class, and/or, posted on the course website.

ii) Electronic versions of all deliverables are due by their posted deadlines according to submission instructions posted on the course website.

5. Teamwork & Group Configurations:

The case analysis components (see below) will be completed as part of a ***workgroup with 6 students***. It is recommended that students setup their own groups. Workgroups must be self-selected during the first two weeks of classes. If any individuals find themselves without groups during week 2, I will form one or two ad hoc group(s) and/or explore some other alternative(s). ***All workgroups are required to submit their team rosters in the form of a memo via email to me by November 5th***. The memo should include student names and email addresses of all members and it should also identify ***a designated group leader*** who will serve as the primary point of contact for the instructor to communicate with the group. For purposes of ensuring privacy, please ***do not disclose your student numbers to other team members***.

6. Performance Evaluation:

The course grading scheme comprises of several components highlighted herewith, alongside their relevant weights. A description of each component follows in the next section.

Components	Responsibility		Tasks & Deliverables	Weight	
	Individual	Workgroup			
Case Discussion Forum		●	Principal Consultant Presentation (Case Discussion Forum)	20%	25%
			Challenge Consultant Review (Case Discussion Forum)	5%	
Technology Tool Pilot Assignment	●		Tool based Mini-Exercises & Worksheet Responses	20%	20%
Participation & Contribution	●		Lecture Discussions & Course Contribution including Case Discussions	10%	10%
Take-Home Final Exam	●		Take-Home Final Exam	45%	45%
					$\sum = 100\%$

7. Performance Evaluation Components:

7.1 Case Discussion Forum *(Workgroup)*

Case studies pertinent to security related subject areas will either be posted on the course website or handed out in class during the second week of classes. Two cases will be assigned to each workgroup such that each workgroup will analyze one case assuming the role of Principal consultants and the second case as Challenge Consultants. While the challenge consultant case for each group will be assigned by the instructor, each workgroup can select their principal case (assigned on first-come basis). The instructor and the rest of the class will act as audience and offer their own insights and ask questions of either consulting teams. As ***Principal Consultants***, the workgroup's assignment will be to: i) thoroughly investigate the details of the selected case, ii) conduct additional pertinent research to formulate their opinion and insights about the case, and iii) present the analysis and recommendations along with justification and accompanying implementation proposals for the problems identified in the case. On the other hand, the ***Challenge Consultants*** will explore the case within the context of course topics and classroom discussions with little external additional research. The challenge consultants will engender their own ideas and offer additional insights following their contender's discussion with the objective of: i) asking suitable questions subsequent to the Principal Consultants presentation, and ii) offering alternative viewpoints and providing a basis for captivating discussions during the case discussion forum.

During each ***case discussion forum***, a maximum of *20 minutes* will be allocated to the Principal Consultants team for their formal presentation followed by a maximum of *10 minutes* of discussion with the Challenge Consultants and a maximum of *5 minutes* of general questions from the instructor and the class audience.

7.2 Technology Tool Pilot Assignment *(Individual)*

In addition to providing a managerial overview of security processes, planning models and technologies that enable secure operational infrastructures, the course also aims to instill a basic practical understanding of technology tools and functional software applications. Towards this, the technology tool pilot assignment is designed to provide ***an assisted overview* of a select set of software applications and tools**. The assignments will be completed on an individual basis. Assignment requirements will be posted on the course website, along with links to relevant sources of information and tutorials to help complete the tasks outlined for the assignment deliverables.

7.3 Participation & Contribution *(Individual)*

Active class participation is a crucial component of your potential grade in this course. Quality input and constructive discussions are encouraged to facilitate an intellectually engaging and interesting learning environment.

The participation grade that you will earn will be a combination of several in-class activities including your involvement as audience and panels in case discussions, meaningful participation in lecture seminars, and your individual contribution in relating experiences, course readings and news items to the discussion themes.

During each lecture, I will make a note of students' participation based on their contribution to class discussions using the following 5-point scheme. A total of 10 points during the course will translate into the maximum 10% devoted to class participation.

0	Student Not in Attendance
1	Student Attended Class
2	Student Ready to Contribute to Discussion in Meaningful Manner
3	Student Related Relevant Personal / Work Experiences or Provided Supplementary Information
4	Student Discussed Pertinent Domain Applications and Provided Useful Examples

7.4 Take-Home Final Exam *(Individual)*

The final exam will be posted online, and will be comprehensive across all course topics including assigned course readings, lecture notes, discussion supplements, research takeaways and other supplementary material. The exam will consist of a combination of multiple choice questions, short answer questions, technology evaluation questions, and mini-case based questions. Each student is individually responsible for completing his/her own exam and submitting it according to posted instructions.

8. Key Course Administration Matters:

8.1 Special Needs & Accessible Learning

Students with disabilities or special needs are advised to contact the University's SASS (Student Academic Success Service) Access Service (e-mail: adapt@uOttawa.ca) for information regarding its services and resources. Students are encouraged to review the calendar for information regarding all services available on campus.

8.2 Class Attendance & Decorum

The teaching method in the course includes class lectures, group discussions, guest lectures, and student presentations. Students are required to attend and participate in all classes. If you must miss a class, please inform me before the class (an e-mail comes in especially handy in helping me keep track of your class participation). Also, if the absence means you will miss a case discussion class, an assignment deadline, or a class presentation, you should make alternative arrangements with your group and also inform me well in advance of the class to be missed.

Your actions in the classroom environment should demonstrate intellectual engagement in the course content, and as well respect for your classmates and for your instructor. As such, talking audibly, reading the newspaper, using cell phones and laptops for chatting and messaging, and other similar disruptions to the learning environment will not be tolerated, and failure to comply with this policy can lead to disciplinary action, up to and including referral to university judiciaries.

8.3 Deadlines for Deliverables & Statute of Limitations

The dates on which assignments are due will be openly published and you are expected, under normal circumstances, to accept responsibility for organizing your affairs to meet the set deadlines. In general, since this is a six-week course, ***late assignments will NOT be accepted***. Extensions for an assignment may be granted in extenuating circumstances, and if you really have a legitimate reason for being late, please contact me BEFORE the due date, so something can be worked out.

Assignment and presentation evaluations will be made available online and/or in-class to the appropriate groups. If you believe that errors were made in assessment or marking, please provide me with the original evaluation along with a short explanation of your objections. The deadline for this is one week after the date on which your assignment was made available to you or your group.

8.4 Academic Integrity

Academic Regulation 14 defines academic fraud as "*any act by a student that may result in a distorted academic evaluation for that student or another student. Academic fraud includes but is not limited to activities such as:*

a) *Plagiarism or cheating in any way;*
b) *Submitting work not partially or fully the student's own, excluding properly cited quotations and references. Such work includes assignments, essays, tests, exams, research reports and theses, regardless of whether the work is written, oral or another form;*
c) *Presenting research data that are forged, falsified or fabricated;*
d) *Attributing a statement of fact or reference to a fabricated source;*
e) *Submitting the same work or a large part of the same piece of work in more than one course, or a thesis or any other piece of work submitted elsewhere without the prior approval of the appropriate professors or academic units;*
f) *Falsifying or misrepresenting an academic evaluation, using a forged or altered supporting document or facilitating the use of such a document;*
g) *Taking any action aimed at falsifying an academic evaluation.*"[1]

The Telfer School of Management does not tolerate academic fraud. Please familiarize yourself with the guidance provided at: http://web5.uottawa.ca/mcs-smc/academicintegrity/home.php

Finally, the Telfer School of Management asks that students sign and submit with their deliverables the Personal Ethics Agreement form. Two versions of this form exist: one for individual assignments, and one for group submissions. **Assignments will not be accepted or marked if this form is not submitted and signed by all authors of the work.** We hope that by making this personal commitment, all students will understand the importance the School places on maintaining the highest standards of academic integrity.

[1] https://www.uottawa.ca/administration-and-governance/academic-regulation-14-other-important-information

Personal Ethics Statement Concerning Telfer School Assignments

Group Assignment:

By signing this Statement, I am attesting to the fact that I have reviewed not only my own work, but the work of my colleagues, in its entirety.

I attest to the fact that my own work in this project meets all of the rules of quotation and referencing in use at the Telfer School of Management at the University of Ottawa, as well as adheres to the fraud policies as outlined in the Academic Regulations in the University's Undergraduate Studies Calendar. Academic Fraud Webpage

To the best of my knowledge, I also believe that each of my group colleagues has also met the rules of quotation and referencing aforementioned in this Statement.

I understand that if my group assignment is submitted without a signed copy of this Personal Ethics Statement from each group member, it will be interpreted by the Telfer School that the missing student(s) signature is confirmation of non-participation of the aforementioned student(s) in the required work.

Signature	Date
Last Name (print), First Name (print)	Student Number
Signature	Date
Last Name (print), First Name (print)	Student Number
Signature	Date
Last Name (print), First Name (print)	Student Number
Signature	Date
Last Name (print), First Name (print)	Student Number
Signature	Date
Last Name (print), First Name (print)	Student Number
Signature	Date
Last Name (print), First Name (print)	Student Number

Statement of Academic Integrity

By signing this Statement, you, the undersigned confirm that this submitted work complies with the rules of academic integrity of the University of Ottawa. Furthermore, you attest to the fact that you have reviewed the entirety of your submitted work, and you have applied appropriate rules of quotation and referencing, as well as adhered to the policies outlined in the University's Academic Regulations as outlined in various resources such as:

- *Academic Integrity: Student's Guide:* http://www.uottawa.ca/vice-president-academic/sites/www.uottawa.ca.vice-president-academic/files/academic-integrity-students-guide.pdf

- *Academic Regulation I-14 (Academic Fraud):* http://www.uottawa.ca/administration-and-governance/academic-regulation-14-other-important-information

Signature _____ Date _____

Last Name (print), First Name (print) _____ Student Number _____