UNSW Business School

School of Information Systems and Technology Management

INFS5907
Security and Ethics in CyberspaceE

Course Outline
Semester 2, 2017

Course-Specific Information

The Business School expects that you are familiar with the contents of this course outline. You must also be familiar with the Course Outlines Policies webpage which contains key information on:

- Program Learning Goals and Outcomes
- Academic Integrity and Plagiarism
- Student Responsibilities and Conduct
- Special Consideration
- Student Support and Resources

This webpage can be found on the Business School website:
https://www.business.unsw.edu.au/degrees-courses/course-outlines/policies

Table of Contents

COURSE-SPECIFIC INFORMATION

1 STAFF CONTACT DETAILS

Position	Name	Email	Room	Phone	Consultation
Lecturer-in-charge	Dr Lesley Land	l.land@unsw.edu.au	QUAD2099A	9385 4738	TBA

2 COURSE DETAILS

2.1 Teaching Times and Locations

Lectures start in Week 1(to Week 12): The Time and Location are:
Mon 6-9 Quadrangle G053 (K-E15-G053).

2.2 Units of Credit

The course is worth 6 units of credit.

2.3 Summary of Course

This course introduces students to the awareness and knowledge of IS/IT security related issues occurring in cyberspace. It has a specific emphasis on the need for ethical viewpoints, approaches and practices from a management perspective when addressing the multidimensional challenges and solutions posed by the IS/IT related security problems. The class will be conducted in a semi-formal workshop fashion. Using business cases and scenarios addressing various cyberspace issues, students will study and discuss the ethical and related implications these issues pose to stakeholders. They will learn to manage cyber related security issues responsibly from ethical, social, corporate, responsible management, and professional perspectives. In some situations, they may encounter dilemmas which require a careful balance and trade-off in the way decisions are made. The course website is maintained on Moodle (see Section 5).

2.4 Course Aims and Relationship to Other Course

This course aims to review concepts, theory, methodologies and techniques discussed in the IS security and ethics literature. In particular, it emphasises the importance of planning, managing decision making in IS security using ethical and related considerations. This course has as prerequisite either INFS5885 or INFS5978 or enrolment in Program 8425 or 8435 or 8426.

2.5 Student Learning Outcomes

The learning outcomes for this course include:

1. Identify the key concepts, theory and practice underlying ethics management in business.
2. Identify the key concepts, theory, methodologies and practice in IS security.
3. Examine current practice for IS security design and implementation to organisational scenarios.
4. Assess IS Security practice – the techniques and methods for securing an organization's information assets.
5. Discuss current research efforts in IS security and ethics.

6. Propose improved security practices to a particular organisational security scenario using ethical considerations.
7. Determine the impact of IS security on organizations and society, including ethical impact.
8. Analyse ethical decision-making using IS security scenarios

The Course Learning Outcomes are what you should be able to DO by the end of this course if you participate fully in learning activities and successfully complete the assessment items.

The Learning Outcomes in this course also help you to achieve some of the overall Program Learning Goals and Outcomes for all undergraduate coursework students in the Business School. Program Learning Goals are what we want you to BE or HAVE by the time you successfully complete your degree (e.g. 'be an effective team player'). You demonstrate this by achieving specific Program Learning Outcomes – what you are able to DO by the end of your degree (e.g. participate collaboratively and responsibly in teams').

For more information on Program Learning Goals and Outcomes, see the School's Course Outlines Policies webpage available at https://www.business.unsw.edu.au/degrees-courses/course-outlines/policies.

The following table shows how your Course Learning Outcomes relate to the overall Program Learning Goals and Outcomes, and indicates where these are assessed (they may also be developed in tutorials and other activities):

Program Learning Goals and Outcomes		**Course Learning Outcomes**	**Course Assessment Item**
This course helps you to achieve the following learning goals for all Business postgraduate coursework students:		*On successful completion of the course, you should be able to:*	*This learning outcome will be assessed in the following items:*
1	Knowledge	Identify the key concepts, theory and methodologies underlying IS security. Examine current methodologies for IS security design and implementation to organisational scenarios.	• Individual assignment • Group assignment • Exam
2	Critical thinking and problem solving	Assess IS security practice - the techniques and methods for securing an organization's information assets. Investigate current IS security methods through web-based research. Propose improved security practices to a particular organisational security scenario. Discuss current research efforts in IS security.	• Class participation • Individual assignment • Group assignment • Exam

		Determine the impact of IS security on organizations and society.	
3a	Written communication	Construct written work which is logically and professionally presented.	Quality of the written individual and group assignment reports.
3b	Oral communication	Communicate ideas in a succinct and clear manner.	Quality of the oral communication for assignments
4	Teamwork	Work collaboratively to complete a task.	Not specifically assessed but a report on group process (reporting on group planning, execution, strengths, weaknesses, conflict resolution, evidences of collaboration etc) must be submitted with the group assignment report. Missing or insufficient reporting will result in a mark deduction. Confidential peer assessment will be utilised to assess equality in the contributions of group members within each group.
5a	Ethical, social and environmental responsibility	Identify and assess possible ethical, environmental and sustainability responsibility considerations in IS security problems in organizational, national and international contexts.	Wherever relevant in case analysis: • Individual and group assignments • Exam
5b	Social and cultural awareness	Identify and assess need for social and cultural awareness in specific case scenarios. For example, successful formulation of organizational standards and for organizational training, social and cultural awareness are important for IS security.	Wherever relevant in case analysis: • Individual and group assignments • Exam

3 LEARNING AND TEACHING ACTIVITIES

3.1 Approach to Learning and Teaching in the Course

This course is developed and delivered within the context of the following learning and teaching philosophy.

In addition to students learning the fundamental content of the course, the content is designed to foster critical thinking and to facilitate the acquisition of life-long learning skills. The course and its delivery are designed with a view to assisting the development

of problem solving skills. The role of the lecturer/tutor of a course is to facilitate learning. It is recognised that students are individuals who bring a diverse range of experiences, interests and abilities and that these aspects of the student will influence their own learning. The responsibility for learning lies with the student. The role of the lecturer/tutor then, is to provide the environment within which students can participate and contribute, interact and experiment while adding to their own skills and knowledge. An important element of such an environment is that students are encouraged to engage in cooperative learning in an enjoyable setting.

Within the context of this philosophy, students will be encouraged to participate, reflect on the material and to engage in meaningful debate with respect to the topics covered. It is essential that students prepare prior to workshops so that they are in a position to contribute to the class discussions. One of the interesting aspects of information and communication technology studies is that there is rarely, if ever, one irrefutable correct answer to a problem – often the only answer is 'depends'. Students are encouraged to investigate and explore the contexts within which certain courses of action are preferable to others and to consider the situation where the best technical solution may not necessarily be the best solution given the constraints of the case at hand.

Accordingly, assessment is weighted toward informed, reasoned and well-argued personal opinion based on the contextual factors and constraints presented in the various scenarios and is consequently, not based on the acquisition of knowledge alone.

3.2 Learning Activities and Teaching Strategies

Learning takes many different forms within this course. The course has a number of topics which are addressed across the twelve weeks of the course. Each topic involves a set of required readings (including the textbook, case studies, and/or papers). Each class will be conducted in a workshop fashion, consisting of a formal lecture, class activities (e.g. discussions or debates) based on a given topic/paper/case study. Students would benefit most from these sessions if they come prepared with the assigned readings and/or preparation. In addition to the textbook and provided slides which form the backbone of the course, case studies which are built on realistic business situations, form an important avenue for helping students grasp with decision making on a variety of IS security issues and they also provide illustrations of specific outcomes within the context. Students will have an opportunity to realise the complexity of the real business environment and hence gain some knowledge on the different ways to tackle business scenarios via discussions. Other materials used in the course include research articles (for informing about the latest research findings in the area), and media articles (for informing about the latest security incidences such as security breaches or changes in security policies/standards). The examination and assessments will assume you are familiar with any of these materials highlighted during the course.

4 ASSESSMENT

4.1 Formal Requirements

To receive a pass grade in this course, you must meet **ALL** of the following criteria:

- attain an overall mark of least 50%;
- attend at least 80% of all scheduled classes;
- attain a satisfactory performance in each component of the course. A mark of 45% or higher is normally regarded as satisfactory;

- attain a mark of at least 45% in the final exam;

In the case of peer assessed group work, the mark assigned to each member of the group may be scaled based on peer assessment of each member's contribution to the task.

4.2 Assessment Details

Assessment in this course is based on workshop participation, an individual quiz, a group assignment and a formal closed book examination. The date for submission of the assignment is also provided in the Workshop Schedule presented at the end of this course outline. An assessment rubric will be published in the assignment specifications.

Assessment Task	**Weighting**	**Length**	**Due Date**
Workshop attendance and participation	10%	-	Ongoing
Individual Quiz	15%	1 hour	Week 6 workshop time 28 August
Group Assignment	25%	Maximum 20 pages and presentation*	Start of Week 11 workshop 9 October
Final Examination	50%	Format TBA	University Exam Period
Total	100%		

* Number of pages contains just the body of the report. It excludes title page, table of contents, references, and appendices.

Additional information will be provided in the individual quiz and group assignment specifications which will be available on the course website.

4.3 Assessment Format

Individual Quiz and Group assignment

The format of the individual quiz will be informed in Week 2.

Additional information on the assessments (e.g. format, style and submission procedure) will be provided in the group assignment specification which will be available on the course website.

The group assignment includes a verbal presentation component. The rubric for the presentation component of the assignment is provided in the Assignment Specification. Please note that the group assignment will be subject to peer review. It is possible that group members within each group could get different marks if individual contributions are not equal. The final mark is left to the discretion of the lecturer.

Workshop Attendance and Participation
Your attendance and participation in the workshop will be monitored throughout the semester. You are expected to prepare and actively participate in both activities. The assessment Rubric for workshop attendance and participations is shown in the table below:

Assessment Rubric for Workshop Participations

Mark	Conditions for which it will be awarded
0 (Unacceptable)	Below 80% of workshop attendance as required by school.
1 – 2 (Very poor)	Minimal to no preparation and participation in the workshop during the semester.
2.5 – 4.5 (Poor)	Generally, poor preparation and participation in workshop during the semester.
5 – 7 (Fair)	Overall average preparation and some participation in workshop discussions in some weeks.
7.5 – 9 (Good)	Overall good preparation and active participation in workshop discussions in most instances.
9.5-10 (Excellent)	Has completed satisfactorily all assigned readings and homework. In addition, demonstrate excellent preparation and very active and thoughtful participation in workshop discussions.

Notes:

* You must attend at least 10 workshops to avoid a 0 mark.
* If a student misses a class due to illness, please produce a valid document to the staff.

4.4 Assignment Submission Procedure

Homework should be submitted in hardcopies when requested (usually the week after release, at the beginning of the workshop).

The individual quiz will be handwritten in class and will be handed in at the end of the hour.

The group assignment must be submitted online using Turnitin in Moodle.

4.5 Special Consideration, Late Submission and Penalties

The late submission of assignments carries a penalty of 10% of the maximum marks for that assignment per day of lateness (including weekends and public holidays), unless an extension of time has been granted. An extension of time to complete an assignment may be granted by the course co-ordinator in case of misadventure or illness. *Applications for an extension of time should be made to the course co-ordinator by email or in person. You will be required to substantiate your application with appropriate documentary evidence such as medical certificates, accident reports etc.* Please note that work commitments, competing deadlines of assignments from other courses, and computer failures are usually consider insufficient grounds for an extension.

For information on Special Consideration please refer to the Business School's Course Outlines Policies webpage**.**

4.6 Protocol for viewing final exam scripts

The School of Information Systems and Technology Management (ISTM) has set a protocol under which students may view their final exam script. ISTM exam script viewing day is usually a day after the official release of results. Details will be posted on both the school website and on your course Moodle.

Quality Assurance
The Business School is actively monitoring student learning and quality of the student experience in all its programs. A random selection of completed assessment tasks may be used for quality assurance, such as to determine the extent to which program learning goals are being achieved. The information is required for accreditation purposes, and aggregated findings will be used to inform changes aimed at improving the quality of Business School programs. All material used for such processes will be treated as confidential.

5 COURSE RESOURCES

The website for this course is on Moodle at:
http://moodle.telt.unsw.edu.au.

All workshop slides and materials will be found on the course website. If only references to papers are provided, you should be able to find the papers in the online UNSW library.

The recommended textbook which should be available in the UNSW bookshop is:

Michael Whitman and Herbert Mattord (2017). *Management of Information Security*, 5th edition, Cengage Learning, Boston, MA, USA.

Michael Whitman and Herbert J Mattord (2014). *Management of Information Security*, 4th edition, Cengage Learning, Thomson Course Technology.

Earlier edition (4th) of the book is also acceptable. However, you will bear the responsibility of ensuring you are aware of changes to the new edition.

The following websites are also useful sources:
http://www.instituteforadvancedsecurity.com/
http://www.auscert.org.au/

6 COURSE EVALUATION AND DEVELOPMENT

Each year feedback is sought from students and other stakeholders about the courses offered in the School and continual improvements are made based on this feedback. UNSW's myExperience is one of the ways in which student evaluative feedback is gathered. In this course, we will seek your feedback primarily through end of semester myExperience evaluations. However, please don't hesitate to give feedback anytime during the semester either verbally or via email to staff. Feedback from previous students indicated that students preferred written feedback. They also preferred lectures to be shorter. As a result of this feedback, written feedback will be given, and lectures will be shorter and more informal, and the lecturer will use more Harvard Business Cases and research/practitioner papers to initiate discussions about different security topics.

7 COURSE SCHEDULE

This schedule is subject to change.

WORKSHOP SCHEDULE		
Week	Topic	
Week 1 24 July	Intro to IS Security and Ethics	
Week 2 31 July	Risk Management (Dr Ken Stevens)	
Week 3 7 August	Ethical Business and Ethics Management Origins of Business Ethics	
Week 4 14 August	Basic Concepts of Business Ethics	
Week 5 21 August	Domains of Business Ethics	
Week 6 28 August	Risk Assessment	Individual In Class Quiz (1 hr)
Week 7 4 September	Risk Control	
Week 8 11 September	IS Policies (Dr Ken Stevens)	
Week 9 18 September	Contingency Planning (Dr Ken Stevens)	
Mid-semester break: 23 September – 2 October inclusive (2 Oct = Labour Day Public Holiday)		
Week 10 3 October	*(Monday 2 October is Labour Day public holiday)*	
Week 11 9 October	Applying ethical practices to IS Security – Case discussions (Dr Ken Stevens)	Group Assignment Due 9 October Group Presentations
Week 12 16 October	Future of Cyber Risks	Group Presentations
Week 13 23 October	Revision	