School of Information Management

MMIM577 Information Security

Trimester Two 2009

COURSE OUTLINE

Names and Contact Details
Course Coordinator
Robert Willison
EA 207
04 463 7436
robert.willison@vuw.ac.nz

Course Administrator
Tiso Ross
EA 121
04 463 5309
tiso.ross@vuw.ac.nz

Trimester Dates
13th July 2009 – 13th November 2009

Withdrawal dates: Information available via
http://www.victoria.ac.nz/home/admisenrol/payments/withdrawlsrefunds.aspx

Class Times and Room Numbers
Trimester dates 13 Jul 09 to 13 Nov 09
Class dates 16/7, 23/7, 30/7, 6/8, 13/8, 20/8, 10/9, 17/9, 24/9.
Day Thursdays
Time 19.40 pm to 21.30pm
Venue RWW414
Class dates 27/8 and 3/9
Day Thursdays
Time 17.40 pm to 21.30pm
Venue RWW413

Course Content
For many organisations, the source of their competitive advantage is now based on the information which they use. A major concern, therefore, is the myriad of threats to such information. If a threat is realised there is the possibility that an organisation could loose its competitive advantage. Hence, information security is now considered a key organisational function. But how do you manage information security? As the use of computer has changed, so too has the security agenda. Securing the early mainframes posed few problems, but as computing power has devolved through and between organisations, the security agenda...
has become far more complex. Adding to this complexity is the central role that all organisational staff play in enforcing security. The aim of this course, therefore, is to equip students with a sound knowledge of information security and how it is managed. By concentrating on managerial aspects, the course aims to provide students with an in-depth knowledge of the non-technical aspects of IS Security, which are vital for conceptualising security (and hence enforcing it) in a coherent manner. The following areas will be covered in the course lectures:

- The changing nature of information security risks.
- Models and concepts for information security management.
- Theory and information security management.
- International security standards.
- Security policies and security education.
- Security technologies.
- Hacking and social engineering (a non technical method for acquiring information).
- The ‘insider’ threat: Employee computer abuse (Part one).
- The ‘insider’ threat: Employee computer abuse (Part two).
- Organisational culture and information security.
- N.B. The course will include two revision lectures.

**Course Learning Objectives**
The course learning objectives include the following:
- Analyse and evaluate theories, concepts and ideas related to information security.
- Assess the utility of relevant theories for application to your own workplace environment.
- Appreciate the need for addressing information security from a socio-technical perspective.
- Understand those elements which constitute information security.
- Convey key information security concepts concisely in an appropriate written format.
- Display articulate oral communication skills.

**Course Delivery**
A series of lectures will act as the foundation for the course. However, in an attempt to provide a more interactive learning environment, students will be involved in class exercises, group presentations and Q&A sessions. These activities will help to engender the themes and concepts addressed in the lectures.

**Expected Workload**
Over the period of the course it is expected that each student will spend the following number of hours on each task:
- Attending lectures: 24 hrs
- Reading the course literature: 36 hrs
- Assignment two: 25hrs
- Assignment three: 15 hours
• Assignment four: 50 hours

N.B. Assignment one relates to class participations and forms 10% of the total course mark. See ‘Assessment Requirements’ for further details.

Group Work
As part of the course, students will be assigned a case study which will be undertaken in groups. This assignment will form 25% of the total course mark.

Readings
Please note that all the course readings will be made available via the ‘Blackboard’ system.


*Theory and Information Security Management.*


*International Security Standards.*


**Security Policies and Security Education.**


**Security Technologies.**


**Hacking and Social Engineering.**


**The ‘Insider Threat’: Employee Computer Abuse (Part One).**


**The ‘Insider Threat’: Employee Computer Abuse (Part Two).**


Organisational Culture and Security


N.B. As stated in the ‘Course Content’ section, there will be two revision lectures.

Assessment Requirements
This course is internally assessed. All assignments are aimed at addressing one or more of the course learning objectives (see above for ‘Course Learning Objectives’).

- Assignment One: Class participation (10%). Students will be assessed during the length of the course in terms of their participation and contribution to the class.

- Assignment Two: Mid-term Group case study (25%) Students will be assigned a mid-term case study project. The case study will be undertaken in groups and will cover some of the lecture material addressed in the first half of the course.

- Assignment Three: Individual Class Presentation and 1000 word report (15%) Students will be assigned a paper to present in class, and present a thousand word summary to the lecturer.

- Assignment Four: Individual Case study analysis in the form of a 4000 word report (50%) Students will be assigned a case study for analysis and expected to hand in a 4000 word report.

Note: Your assessed work may also be used for quality assurance purposes, such as to assess the level of achievement of learning objectives as required for accreditation and audit purposes. The findings may be used to inform changes aimed at improving the quality of FCA programmes. All
material used for such processes will be treated as confidential, and the outcome will not affect your grade for the course.

Penalties
In keeping with standards of professionalism, it is expected that deadlines, time limits and word counts will be adhered to. Late submissions are not acceptable unless they have been agreed with the coordinator prior to the date on which they are due. Unsignalled lateness will result in the available marks being reduced by 5% per day.

Mandatory Course Requirements
Students must submit all required assessments and obtain a total mark of ‘C’ to pass the course. Grading schedule: 85-100% A+; 80-84% A; 75-79% A-; 70-74% B+; 65-69% B; 60-64% B-, 55-59% C+; 50-54% C (pass grade); 40-49% D; 0-40% E.

Communication of Additional Information
Course information will be conveyed to the students via the ‘Blackboard’ system.

Use of Turnitin (if applicable)
Student work provided for assessment in this course may be checked for academic integrity by the electronic search engine http://www.turnitin.com. Turnitin is an on-line database of existing material. At the discretion of the Head of the School, handwritten work may be copy-typed by the School and subject to checking by Turnitin. Turnitin will retain a copy of submitted material on behalf of the University for detection of future plagiarism, but access to the full text of submissions will not be made available to any other party.

For the following important information follow the links provided:

Academic Integrity and Plagiarism
http://www.victoria.ac.nz/home/study/plagiarism.aspx

General University Policies and Statutes
http://www.victoria.ac.nz/home/about/policy/academic.aspx

Faculty of Commerce and Administration Offices
http://www.victoria.ac.nz/fca/studenthelp/Contactus.aspx

Manaaki Phipihinga Programme
http://www.victoria.ac.nz/st_services/mentoring/