TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

School of Information Management

# MMIM 577 INFORMATION SECURITY

Trimester 1, 2016

## COURSE OUTLINE

---

**Contact Details**

| | |
|---|---|
| **Course Coordinator & Lecturer:** | Assoc. Prof. Val Hooper<br>Room: RH 525<br>Phone: (04) 463-5020<br>E-mail: val.hooper@vuw.ac.nz<br>Office hours: By appointment |
| **Lecturer:** | Jeremy McKissack<br>Room: RH 414<br>Phone: (04) 463-5233 ext. 6876<br>Email: jeremy.mckissack@vuw.ac.nz<br>Office hours: By appointment |
| **Programme Administrator:** | Usha Varatharaju<br>RH 520, Level 5, Rutherford House, Wellington<br>Phone: (04) 463 5309<br>e-mail: usha.varatharaju@vuw.ac.nz |
| **Trimester Dates:** | Monday 4 April – Friday 3 June |
| **Class Times:** | Thursday 5.40pm – 8.30pm |
| **Venue:** | **AM 103**, Alan MacDiarmid Building, Room 103, Kelburn Campus and **KS50/410**, 50 Kitchener St, Room 410, Auckland campus |

**Withdrawal from Course**

1. Your fees will be refunded if you withdraw from this course on or before Friday 15 April 2016.

2. The standard last date for withdrawal from this course is Friday 20 May 2016. After this date, students forced to withdraw by circumstances beyond their control must apply for permission on an '*Application for Associate Dean's Permission to Withdraw Late'* including supporting documentation. The application form is available from either of the Faculty's Student Customer Service Desks or online.

**Prescription**

An up-to-date survey of information security developments. Topics may include authentication, access control, intrusion detection, malicious software, and firewalls; human factors, security auditing, IT security management and risk assessment, and internet security protocols and standards.

## Course Learning Objectives

Security and risk have become crucial to the management and use of information and information systems. Issues include an understanding of the risks associated with information systems security, why they are a matter for concern across all levels of the organisation, how risk and security assessments should be done in terms of impact on systems integrity, impact on systems, impact on staff, impact on reputation and on market share.

More specifically stated the course objectives are to

1. Help students understand and appreciate information security threats, vulnerabilities and impacts arising from the use of information systems to support business processes.
2. Consider the implications of system and network vulnerability in the context of business strategy, strategic risk management and IT governance.
3. Provide a conceptual management framework with which to address information security risks in a coherent and structured manner (*e.g*. how to assess the suitability of security controls proposed for a new business IT system; how to balance potential security impacts against the costs of control).
4. Relate theory to practice through the use of case studies and classroom discussion based on real world experience of information security management.

Please note that this is not a course in the technology of information systems security. It is a management course intended to sensitize students to security and risk issues that impact on management considerations in an information age. On completion of the course students will, however, have a good understanding of the building blocks of corporate information systems, how those blocks fit together, and how they need to be protected.

### Learning Outcomes

By the end of this course students should be able to:

1. Undertake library and internet research and record their findings according to standard academic requirements.
2. Understand some of the important philosophical, technical and commercial principles underpinning information security risks, practices and controls.
3. Evaluate the business opportunities and limitations that information security risk place upon managers.
4. Appreciate the use of information security within an organisation's risk management practice and general governance framework.
5. Discuss intelligently information security risk and control issues in Information Management.

## Course Content

The course will be delivered in seminar form with in class discussions, group work as well as lectures. Modules will more or less equate to lectures, depending on progress made each week.

| Class | Date | Topic | Deliverables | % |
|---|---|---|---|---|
| 1 | 7 April | Introduction<br>Defining security and main concepts; Threats | | |
| 2 | 14 April | Risks | SPA 1 | 5% |
| 3 | 21 April | Frameworks and architecture | SPA 2 | 5% |
| 4 | 5 May | Governance and compliance | SPA 3 | 5% |
| 5 | 12 May | Information protection and privacy | SPA 4<br>Group presentation: Risk Management | 5%<br>15% |
| 6 | 19 May | Security awareness | SPA 5 | 5% |
| 7 | 26 May | Physical security and disaster recovery | SPA 6<br>Group presentation: Security improvement plans | 5%<br>15% |
| 8 | 2 June | | Test | 40% |

## Course Delivery

The course will be delivered in face-to-face and distance class sessions. The sessions will comprise lectures and discussions on each week's topics. There will be opportunity for two group presentations and one in-class test.

## Readings

**Week 1 Defining security and main concepts; Threats (7 April)**
**Week 2 Risk (14 April)**
**Week 3 Frameworks and architecture (21 April)**
**Week 4 Governance and compliance (5 May)**
**Week 5 Information protection and privacy (12 May)**

Dinev, T., Xu, H., Smith, J. H. and Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems, 22, 295-316.

Gillon, K., Branz, L., Culnan, M., Dhillon, G., Hodgkinson, R. and MacWillson, A. (2011). Information security and privacy – rethinking governance models. *Communications of the Association for Information Systems*, 28 (33), 561-570.

New Zealand. Human Rights Review Tribunal (2015). NZHRRT 6. Reference No. HRRT 027/2013. Between Karen May Hammond and Credit Union Baywide. Decision of the Tribunal.

**Week 6 Security awareness (19 May)**

Haeussinger, F. J. and Kranz, J. K. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behaviour. *34th International Conference on Information Systems*, 1-16.

Johnston, A. C., Karkentin, M. and Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asses through sanctioning rhetoric. *MIS Quarterly*, 39(1), 113-134.

Willison, R. (2009). *Motivations for employee computer crime: Understanding and addressing workplace disgruntlement through the application of organisational justice.* Department of Informatics, Copenhagen Business School, Working Paper nr 1.

**Week 7 Physical security and disaster recovery (26 May)**

Liang, H. and Xue, Y. (2010). Understanding security behaviours in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.

Puhakainen, P. and Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757-778.

Van Niekerk, J. F. and Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29, 476-486.

Because the topics dealt with change so fast, where appropriate, additional readings might be posted onto Blackboard prior to each lecture. Students will be alerted to these.

The following resources will be useful for students studying this course:

Whitman, M. E. & Mattord, H. J. (2005) *Principles of Information Security*, 3rd ed. Boston, Ma.: Thomson Course Technology. *(This text was previously prescribed within the MIM programme).*

New Zealand Information Security Manual (2010), [online]
http://www.gcsb.govt.nz/newsroom/nzism/NZISM_2011_Version_1.01.pdf
*(Version 2 of the NZISM should be available online later in 2014)*

Security in the Government Sector (2002), [online]
http://www.nzsis.govt.nz/assets/media/Security_in_the_Government_Sector_2002.pdf

Australian Government Information Security Manual (2014), [online]
http://www.asd.gov.au/publications/Information_Security_Manual_2014_Controls.pdf

SANS Institute Reading Room
http://www.sans.org/reading-room

## Assessment

| Assessment Item | % | Learning Outcomes Assessed |
|---|---|---|
| Session Preparation Assignments (6) | 30 | 1, 2, 3, 4, 5 |
| Group projects oral and written (2) | 30 | 1, 2, 3, 4, 5 |
| Final in-class case study/test | 40 | 2, 3, 4, 5 |

Detailed guidelines for each assessment will be distributed to students at the start of the course.

The Assessment Handbook will apply to all VUW courses: see
http://www.victoria.ac.nz/documents/policy/staff-policy/assessment-handbook.pdf

| Pass/Fail | Grade | Normal Range | Indicative Characterisation |
|---|---|---|---|
| Pass | A+ | 90%-100% | Outstanding performance |
| | A | 85%-89% | Excellent performance |
| | A- | 80%-84% | Excellent performance in most respects |
| | B+ | 75%-79% | Very good performance |
| | B | 70%-74% | Good performance |
| | B- | 65%-69% | Good performance overall, but some weaknesses |
| | C+ | 60%-64% | Satisfactory to good performance |
| | C | 55%-59% | Satisfactory performance |
| | C- | 50%-54% | Adequate evidence of learning |
| Fail | D | 40%-49% | Poor performance overall, some evidence of learning |
| | E | 0-39% | Well below the standard required |

Quality Assurance 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 VBS 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 appropriate to this programme, it is expected that deadlines will be honoured. In fairness to students who complete work on time, work submitted after the due date/ time will incur penalties for lateness. The penalty is up to 5 % of the report's grade per day (or part thereof) late. Unusual or unforeseeable circumstances (*e.g.* serious illness, family bereavement) may lead to a waiver of this penalty but need to be discussed with the course coordinator as soon as possible.

Being succinct and staying focused is an important management skill so excessively long assignments will be penalized *pro rata* according to the extent of overrun (*e.g.* 25% score reduction for a paper that is 125% of the stated maximum length).

**Mandatory course requirements**

Students must obtain a minimum mark of 50% for the test in order to pass MMIM 577. The mark obtained contributes 40% to the final overall course mark.

If you believe that exceptional circumstances may prevent you from meeting the mandatory course requirements, contact the Course Coordinator for advice as soon as possible.

If you cannot complete an assignment or sit the test, refer to www.victoria.ac.nz/home/study/exams-and-assessments/aegrotat

**Expected Workload**

A total of 150 hours of work is expected from each student. That consists of approximately 24 hours of classes, and approximately 16 hours per week outside class during teaching weeks and during the break spent reading, studying and writing assignments.

**Group Work**

Students will be required to participate in two group projects. The contribution of each project to the final course mark will be 15% (10% for the written group component, and 5% for the individual oral component). Detailed guidelines will be provided to the students at the start of the course.

**Use of Turnitin**

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 plagiarism prevention tool which compares submitted work with a very large database of existing material. At the discretion of the Head of School, handwritten work may be copy-typed by the School and submitted to Turnitin. A copy of submitted materials will be retained 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.

**Student feedback**

There will be an opportunity for students to provide feedback on both the course and the teaching towards the end of the course.

Student feedback on University courses may be found at www.cad.vuw.ac.nz/feedback/feedback_display.php.

**Communication of Additional Information**

Additional information or information on changes will be announced in class, posted on Blackboard and/or e-mailed to students, depending on the situation. It is imperative that students monitor Blackboard regularly as well as their student e-mail accounts.

**Link to general information**

For general information about course-related matters, go to
http://www.victoria.ac.nz/vbs/studenthelp/general-course-information

**********