Faculty of Information Technology
School of Information Management and Systems
Semester 1, 2005
UNIT OUTLINE

Unit: IMS5002 – Information Systems Security

The Handbook entry for IMS5002 can be found at: http://www.monash.edu.au/pubs/handbooks/subjects/IMS5002.html

Unit webpage: To access unit webpage, select: http://www3.sims.monash.edu.au/subjects/ims5002.nsf

Lecturer: Susan Foster
Room 7.17 (Level 7, Building S, Caulfield Campus)
Phone – 9903 2404
Email – sue.foster@sims.monash.edu.au

Teaching Assistants This will be updated when tutors have been allocated

<table>
<thead>
<tr>
<th>Tutors (TBA)</th>
<th>Room</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>9903 1918</td>
<td></td>
</tr>
</tbody>
</table>

Contacting staff: Outside the scheduled class contact hours, you can contact teaching staff by email, during their consultation hours (available on unit webpage or at SIMS frontdesk) or by making an appointment. If you need a staff member urgently and are unable to contact them, please contact: SIMS Frontdesk, Level 7 – Building S, Ph: 9903 2208

Prerequisites: IMS9001, IMS9003, IMS9049
Prohibitions: SYS3110, SYS3194, SYS4110, IMS3110
Aim

To provide students with the ability to understand and evaluate IS security concepts and their relevance to the management of the IT function in contemporary organisations.

Objectives:

At the completion of this unit the students will:

**have knowledge of:**

- current security philosophies, security methodologies, security analysis and design methods and techniques, security management, and professional ethics

**have an understanding of:**

- the ethical, legal and criminal issues relating to the security of information systems

**have the skills to:**

- apply security analysis and design methods and techniques in the analysis of the threats, risks, and breaches of an information system, and in the design of suitable security control measures.

**have developed attitudes which enable them to:**

- demonstrate ethically sound viewpoints with respect to the protection of information confidentiality, integrity, and availability.

Texts and software:

The following is a list of recommended reading and includes a number of website locations useful for downloading industry and government whitepapers. This list will be added to at different times and will form part of your weekly lecture and tutorials.

If you find an article or book you think is interesting and would be helpful to other students, please email either the lecturer or your tutor and we will publish the reference.

Prescribed resources:

As this is a dynamic subject, there are no prescribed resources. I prefer students to obtain, and have access to a variety of different resources.

Recommended resources:


**On Reserve (Caulfield Library only):**

Students are reminded that books “on reserve” can be obtained from the library counter. Students have access to these books for two hour time slots. You may photocopy articles and resources as required.


**Additional references:**


Important Web sites:
(www.netiq.com)
www.CSOonline.com.au
http://www.cert.org/
http://www.cert.org/archive/html/protect-critical-systems.html#abs
Presentations and reports: Attack and intruder trends
http://www.cert.org/nav/index_red.html
Independent Commission Against Corruption. eCorruption: eCrime vulnerabilities in the
http://www.thinkmobile.com/News/00/48/29/
Disaster Strategies for Record Keeping:
http://www.treasury.gov.au

Developing a security policy, December 2001, SunBluePrints
http://www.sun.com/blueprints

Study materials:

We provide:

- Assignment specifications
- Lecture notes via the unit website
- Additional reading and internet information
Unit structure and organisation:

<table>
<thead>
<tr>
<th>Week</th>
<th>Start date</th>
<th>Lecture Topics</th>
<th>Tutorial topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>28 Feb</td>
<td>Overview of the unit</td>
<td>No tutorials</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security governance</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>7 March</td>
<td>Managing security in the organisation</td>
<td>T1 Lecture review questions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Major Assignment handout</td>
</tr>
<tr>
<td>3</td>
<td>14 March</td>
<td>Risk Management</td>
<td>T2 Group presentations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Breaches, threats, vulnerabilities and controls</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>21 March</td>
<td>IS Security – Access Controls</td>
<td>T3 Group presentations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Friday 25 March to Friday 1 April – Mid semester vacation

<table>
<thead>
<tr>
<th>Week</th>
<th>Start date</th>
<th>Lecture Topics</th>
<th>Tutorial topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>4 April</td>
<td>IS Security – computer forensics</td>
<td>T4 Group presentations</td>
</tr>
<tr>
<td>6</td>
<td>11 April</td>
<td>Impact of e-commerce on the organisation <a href="http://www.cert.org/encyc_article/tocencyc.html">http://www.cert.org/encyc_article/tocencyc.html</a></td>
<td>T5 Tutorial exercise 1 due in (5%)</td>
</tr>
<tr>
<td>8</td>
<td>25 April</td>
<td>Security as a critical business function</td>
<td>T7 Group presentations</td>
</tr>
<tr>
<td>9</td>
<td>2 May</td>
<td>Security policies and procedures</td>
<td>T8 Group presentations</td>
</tr>
<tr>
<td>10</td>
<td>9 May</td>
<td>Business continuity plans/disaster recovery</td>
<td>T9 Group presentations</td>
</tr>
<tr>
<td>11</td>
<td>16 May</td>
<td>Security standards, privacy and law</td>
<td>T10 Major Assignment due in assignment box at 5.00 pm (30%)</td>
</tr>
<tr>
<td>12</td>
<td>23 May</td>
<td>Current issues and Future Trends in IS Security –</td>
<td>T11 Group presentations</td>
</tr>
<tr>
<td>13</td>
<td>30 May</td>
<td>Review and Revision</td>
<td>T12 Group presentations</td>
</tr>
<tr>
<td>14-17</td>
<td>6 June-1 July</td>
<td>Examination period</td>
<td>Revision questions</td>
</tr>
</tbody>
</table>

Workload:
This is a six point unit which, according to University guidelines, requires you to spend 12 hours per week (a total of at least 156 hours per semester).

The anticipated workload is:
- 2 hours per week lecture
- 1 hour per week consultation and discussion
- 6 hours per week assignment work
- 3 hours per week reading
Assessment Notes:

The assignments (50% weighting) and a two hour examination (50% weighting) will be used to assess whether you have achieved the unit objectives.

Your assignments comprise the following assessable items:

- Major assignment 30%
  
  Due date 20 May (hand in by 5 pm in assignment box on level 7, Bldg S)

- Group presentation – topic – IS Security tools 10%

- Tutorial exercises x 2 – topics to be advised 10%

The formal supervised assessment for this unit will be an exam scheduled in the formal examination period following the last week of semester:

- Examination 2 hours (plus 10 minutes reading time), closed book (50%)

You are required to be available for the exam and any necessary supplementary assessment procedures until the end of the assessment period. Alternative times for exams will not be approved without a medical certificate for a significant illness, or equivalent evidence.

Note:

- Assignments in this unit are no less important than those of other units. Your inability to manage your time or computing resources will not be accepted as a valid excuse. (Several assignments falling due at the same time is often unavoidable.)
- Backup copies are required to be made of all assignments and retained for 12 months, in case of loss.
- Hardware failures are not normally recognised as a valid reason for obtaining an extension or handing in a late assignment.

1 Acknowledgment of sources

Each time you complete any assessment, please refer to and make yourself familiar with the most current information regarding acknowledgement of sources, plagiarism and academic conduct contained in the SIMS Policy website.

http://www.sims.monash.edu.au/policies

2. Assignments

2.1 Standards for presentation

All printed assignment work must be word processed and meet the standards set out in the assignment. Refer also to the School of Information Management and Systems guidelines for writing assignments for additional information on presentation standards:


2.2 All assignments must include an appropriate signed SIMS assignment cover page. See the SIMS web site for downloadable (PDF) copies of SIMS assignment cover pages

2.3 Extensions

If you believe that your assignment will be delayed because of circumstances beyond your control such as illness, you should apply for an extension prior to the due date. All applications for extensions must be made in writing to your lecturer. Medical certificates or other supporting documentation will be required.

Late assignments submitted without an approved extension may be accepted (up to one week late) at the discretion of your lecturer, but will be penalised at the rate of 10% of total assignment marks per day (including weekends). Example:

Total marks available for the assignment = 100 marks
Marks received for the assignment = 70 marks
Marks deducted for 2 days late submission (20% of 100) = 20 marks
Final mark received for assignment = 50 marks

2.4 Submission of assignments

All assignments are to be submitted to your tutor during your allocated tutorial. If you are handing in assignments early, please email this intention to your tutor and attach the assignment document and SIMS cover sheet.

2.5 Return of assignments

Assignments will either be returned in specified tutorials during semester or via the SIMS Frontdesk collection system outside semester.

In general, assignments will be returned within two to three weeks of the due date.

3 Student Academic Grievance Procedure

If you have a concern or issue about aspects of your assessment or other academic matters, you are encouraged to follow the SIMS Student Academic Grievance Procedure: http://www.sims.monash.edu.au/resources/index.html

4. Pass requirements

The 40% rule applies to units and determines the final result for a student where the student's performance in either the examination or assignment component of the unit is unsatisfactory. Students need to be aware of the 40% rule which is:

In order to pass a unit, a student must gain all of the following:

- at least 40% of the marks available for the examination component: i.e. the final examination and any tests performed under exam conditions, taken as a whole
- at least 40% of the marks available for the assignment component: i.e. the assignments and any other assessment tasks (such as presentations) taken as a whole
- at least 50% of the total marks for the unit

Where a student gains less than 40% for either the examination or assignment component, the final result for the unit will be no greater than ‘44-N’.
5. **Grades**

The grades awarded by the Faculty of Information Technology are:

<table>
<thead>
<tr>
<th>Grade</th>
<th>Code</th>
<th>Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Distinction</td>
<td>HD</td>
<td>80-100</td>
</tr>
<tr>
<td>Distinction</td>
<td>D</td>
<td>70-79</td>
</tr>
<tr>
<td>Credit</td>
<td>C</td>
<td>60-69</td>
</tr>
<tr>
<td>Pass</td>
<td>P</td>
<td>50-59</td>
</tr>
<tr>
<td>Fail</td>
<td>N</td>
<td>0-49</td>
</tr>
<tr>
<td>Near Pass</td>
<td>NP</td>
<td>45-49 (may be awarded by Board of Examiners only)</td>
</tr>
<tr>
<td>Deferred</td>
<td>DEF</td>
<td>-</td>
</tr>
<tr>
<td>Withheld</td>
<td>WH</td>
<td>-</td>
</tr>
</tbody>
</table>