Faculty of Information Technology
School of Information Management and Systems
Semester 2, 2005
UNIT OUTLINE

Unit: IMS3110, Information Systems Security


The Handbook entry for IMS3110 can be found at:

Unit webpage: To access unit webpage, select:

Staff:

<table>
<thead>
<tr>
<th>Role</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lecturer</td>
<td>Sue Foster</td>
</tr>
<tr>
<td>Room</td>
<td>7.17 Level 7, Building S, Caulfield Campus</td>
</tr>
<tr>
<td>Phone</td>
<td>9903 2404</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:Sue.Foster@sims.monash.edu.au">Sue.Foster@sims.monash.edu.au</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tutors</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Namit Surana</td>
<td><a href="mailto:Namit.surana@infotech.monash.edu.au">Namit.surana@infotech.monash.edu.au</a></td>
</tr>
<tr>
<td>Syie Lum</td>
<td><a href="mailto:Syie.Lum@infotech.monash.edu.au">Syie.Lum@infotech.monash.edu.au</a></td>
</tr>
<tr>
<td>Room</td>
<td>Room T1.03</td>
</tr>
<tr>
<td>Phone</td>
<td>Phone 9903 2631</td>
</tr>
</tbody>
</table>

Contacting staff: Outside the scheduled class contact hours, you can contact teaching staff by email or phone, 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
Aim: This unit is designed to provide students with an understanding and appreciation of a range of information system security components, principles and policies, strategies. Information security philosophies are discussed along with methods, models, techniques and controls, including risk analysis, qualitative and quantitative matrices, and access controls; such as passwords, smart cards, and security auditing. Information security is especially considered in the area of Internet security management and policy; and from the standpoint of ethical and legal issues, as well as computer crime. Information security current issues and future trends will also be discussed.

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 threats, risks, and breaches to 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 resources in regard to maintaining a secure IS framework; in relation to confidentiality, integrity, and availability, in the professional development of information systems

Prerequisite knowledge: Students are required to have completed prerequisite unit CSE1205, IMS1002, SYS1002, SYS2168 or equivalent.

Prohibitions: IMS5002, SYS3194, SYS4110, SYS3110
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.

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. Please DO NOT DEFACE THESE ITEMS BY WRITING OR HIGHLIGHTING areas. These are for all students in this unit.


Recommended resources:


**Important Web sites:**
[www.CSOonline.com.au](http://www.CSOonline.com.au)
Presentations and reports: Attack and intruder trends
[http://www.cert.org/nav/index_red.html](http://www.cert.org/nav/index_red.html)
Disaster Strategies for Record Keeping:
Developing a security policy, December 2001, SunBluePrints

**Additional resource material:**

Although the above resources provide a range of views for this topic area and provide valuable information and resources, no single text is used as the basis for assessment in this unit. Additional reading from a variety of sources provided in class and by personal sourcing should be supplemental to this course.

Therefore students are encouraged to read widely in the business and popular industry press (Computer World, Gartner, Forrester, SANS, AUScert) related to specific issues that reflect topics in this unit.

**Study materials:**

- Weekly PPT slides via the unit website
- Additional reading resources will either be provided on the website, at the end of the slide presentation, or during lectures
<table>
<thead>
<tr>
<th>Week</th>
<th>Date (week beginning)</th>
<th>Lecture Topics</th>
<th>Assessment</th>
<th>Tutorials</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>18 July</td>
<td>Brief overview of the unit and unit outline Introduction to IS Security in organisations</td>
<td>Presentations form part of the assessment and will be carried out in tutorials</td>
<td>No Tutorial this week</td>
</tr>
<tr>
<td>2</td>
<td>25 July</td>
<td>IS Security – framework Breaches, threats, vulnerabilities</td>
<td>Assignment 1 handed out</td>
<td>Introduction to IS security and the goals of IS Security</td>
</tr>
<tr>
<td>3</td>
<td>1 August</td>
<td>IS Security – access controls Andrew Dixon – librarian – talk on accessing databases and electronic journals, referencing internet sources etc. Andrew is SIMS contact person at the library</td>
<td>Breaches, threats, vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>8 August</td>
<td>Risk management</td>
<td></td>
<td>IS Security access controls Presentation 1&amp;2</td>
</tr>
<tr>
<td>5</td>
<td>15 August</td>
<td>Risk analysis</td>
<td>Assignment 1 due = 5%</td>
<td>Risk management</td>
</tr>
<tr>
<td>6</td>
<td>22 August</td>
<td>E-commerce - Internet security</td>
<td></td>
<td>Risk analysis Presentation 3</td>
</tr>
<tr>
<td>7</td>
<td>29 August</td>
<td>Internet security cont/d</td>
<td></td>
<td>E – commerce – internet security Presentation 4</td>
</tr>
<tr>
<td>9</td>
<td>12 September</td>
<td>Security policies and procedures</td>
<td></td>
<td>Security policies etc Presentation 6</td>
</tr>
<tr>
<td>10</td>
<td>19 September</td>
<td>Business continuity plans (BCP) and disaster recovery</td>
<td>Assignment 2 due – 20%</td>
<td>BCP and disaster recovery</td>
</tr>
<tr>
<td></td>
<td>26 September - 30 September</td>
<td>MID SEMESTER BREAK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>3 October</td>
<td>Privacy and the law</td>
<td>Tutorial exercise 5%</td>
<td>Privacy and the law</td>
</tr>
<tr>
<td>12</td>
<td>10 October</td>
<td>Current issues and future Trends in IS Security</td>
<td></td>
<td>Current issues and future trends Presentation 7&amp;8</td>
</tr>
<tr>
<td>13</td>
<td>17 October</td>
<td>Review and Revision Exam Preparation</td>
<td></td>
<td>Review and revision</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 tutorials
- 7 hours per week preparation and assignment
- 2 hours per week reading

Assessment:

The combined assignments (40% weighting) and a two hour examination (60% weighting) will be used to assess whether you have achieved the objectives of this subject.

- Assessments 40% Weighting Due date
  Assign 1 5% Week 5 (in tutorial)
  Assign 2 20% Week 10 (Fri 23/09)
  Assign 3 Presentation 7.5% In tutorials
  Tutorial exercise x1 7.5% Week 12 (in tutorial)
- Final examination 60%

A closed book examination of 2 hours, will be used to test your ability to meet the unit objectives.

Formal supervised assessment
(e.g. The formal supervised assessment for this unit will be an exam scheduled in the formal examination period following the last week of semester. 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.
Assessment Notes

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 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

Assignments should be submitted to your tutor during your allocated tutorial. However, assignments submitted before the due date or outside the allocated tutorial time should be submitted to level 7, S building, IMS3110 assignment drop box by 5pm on the due date. Students who are unsure of due dates for assignments should check their assignment handout sheet, review their unit outline or consult their tutor.

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/policies](http://www.sims.monash.edu.au/policies)

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, if any: 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>