IMS3110 – Information Systems Security

Semester 2, 2005

IMS3110 - MAJOR ASSIGNMENT

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Due Date</th>
<th>Hand in</th>
<th>Mark Allocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment 1</td>
<td>Week beginning Monday, 16 August</td>
<td>During tutorial</td>
<td>5 %</td>
</tr>
<tr>
<td>Assignment 2</td>
<td>Friday, 7 October – 5 pm</td>
<td>IMS3110 Assignment box Level 7, S bldg</td>
<td>20%</td>
</tr>
</tbody>
</table>

**NB: PLEASE DO NOT EMAIL ASSIGNMENTS TO YOUR TUTORS OR MYSELF**

**AIMS**
The aims of the assignment are to:

1. Develop your understanding of information systems security theory and practice
2. Develop the capacity to understand and apply information systems security concepts
3. Develop an understanding of information systems security issues

**ASSIGNMENT PRESENTATION**

a) A word count must be provided.
b) The assignment MUST CLEARLY REFLECT IS SECURITY
c) Assignments that are excessively long or unreasonably short will be penalised.
d) Headings and sub-headings should be used as appropriate.
e) A contents page should be provided.
f) Please DO NOT provide an abstract or an executive summary.
g) Submissions must be word processed and provided in hard copy by the due date.
   (See page 6 of Unit outline regarding SIMS style guide.)
h) All assignments MUST HAVE a SIMS cover sheet, with the student name, ID number, email address etc. See website: (URL: [http://www.sims.monash.edu.au/resources/assessment.html](http://www.sims.monash.edu.au/resources/assessment.html))

If you are uncertain as to the approach your assignment should take please discuss the issues with your lecturer, Susan Foster or your tutor.
ASSIGNMENT 1

STRUCTURE AND OVERVIEW OF ASSIGNMENT 2

Due Date: Week 5
(hand in to your tutor during tutorials)

Mark Allocation: 5%

Word count: approximate length 1000 words

THIS IS TO BE AN INDIVIDUALLY PRESENTED ASSIGNMENT

INSTRUCTIONS:

1. Assignment 1 should be based on Assignment 2. (See page 3 of this handout.)
   a. Provide a brief description of the topic you have chosen
   b. Provide the main topic headings demonstrating the structure of the assignment
      i. under each of these headings describe briefly how the subject matter will
         contribute to developing an evaluation of the topic
      ii. develop links between each new section
      iii. ensure flow and continuity in developing the structure and between each
         new section
   c. Include two or three main references you have sourced to date.
   d. Demonstrate the use of your referencing technique by strategically including
      them in the body of this overview as well as including them in a reference list at
      the end.

NB: If you decide after completing assignment 1 you do not want to pursue the same
topic for Assignment 2, you MUST contact the lecturer or your tutor to discuss the
new topic and decide if this is feasible given the short time frame.
Assignment 2

Due Date: Week 11 – Friday 3 October at 5.00 pm

Hand in: During your allocated tutorial or in IMS5002 assignment box – Level 7 S building by 5.00 pm (the assignment box will be cleared promptly)

DO NOT EMAIL THE ASSIGNMENT

Mark Allocation 20%

Word count approximate length 2,500 - 3000

You may choose one of the following three assignment options:

**Option 1**
This is a specific topic on vulnerability management (see pages 4 – 5)

**Option 2**
You may choose from a range of selected topics. (see page 6)

**Option 3**
is an open topic of your own choosing but this MUST be arranged in advance with your lecturer.

(NB: This is only suitable for students who are working or have access to an organisation and would like to evaluate a certain aspect of the security within the organisation.)

EXTENSIONS AND LATE ASSIGNMENTS

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).

PLAGIARISM AND CHEATING


Plagiarism and Collusion are methods of cheating for the purposes of Monash Statute 4.1 – Discipline

**Plagiarism** is the presentation of work which has been copied in whole or in part from another person's work, or form any other source such as the Internet, published books or periodicals, without due acknowledgement given in the text.

**Collusion** is the presentation of work which is the result in whole or in part of unauthorized collaboration with another person or persons.

All students enrolled in SIMS units must follow the FIT Plagiarism and Cheating policy.

Please ensure that you are familiar with the information, policies and procedures detailed at the following web sites:

Background

Howard F. Lipson, Ph.D., CERT® Coordination Center, 2002 is quoted as saying:

“Perhaps the greatest threat to the Internet today is the abysmal state of security of so many of the systems connected to it. There are many contributing factors, including commercial off-the-shelf (COTS) software, in which the number of features and rapid time to market outweigh a thoughtful security design. New vulnerabilities are continually being discovered in such software. The widespread use of many COTS products means that once a vulnerability is discovered, it can be exploited by attackers who target many of the thousands or even millions of systems that have the vulnerable product installed. A lack of security expertise by most Internet users means that vendor security patches to remove the vulnerabilities will not be applied promptly, if at all. As a result, systems with unpatched vulnerabilities can be easily compromised, in large numbers, by motivated attackers, who will then use these systems as launching points to concentrate an attack against better-protected systems and to hide the tracks of the attacker.”

Your brief:

1. Describe the term vulnerability management (10 marks)
2. Describe the possible impacts to an organisation once a vulnerability has been exploited by a hacker (20 marks)
3. Design a security system that will maximise the ability to manage vulnerabilities in an information system. (You should include the Control Relational model and a Defence in Depth strategy to support your design.) (40 marks)
4. IT staff seem powerless to respond effectively to the increasing security threats impacting on information systems. Provide reasons why this is the case. (15 marks)
5. Presentation and referencing (15 marks)

NB: As part of your answer you should include any other issues that should be considered.
<table>
<thead>
<tr>
<th>REFERENCING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ø 15 references (at least) – no more than 10 references should come from internet sources</td>
</tr>
<tr>
<td>Ø The reference list must be placed at the back of the assignment</td>
</tr>
<tr>
<td>Ø A reference for this assignment means you have used a source to develop your answer and this source must be cited in the body of the paper as well as correctly referenced in the reference list.</td>
</tr>
<tr>
<td>Ø (If you are unsure how to display your references, see SIMS Style Guide which is available on the SIMS website.)</td>
</tr>
</tbody>
</table>

*NB:* Assignments that lack references in the body, but have a comprehensive reference list will be heavily penalised OR NOT MARKED.
ASSIGNMENT 2 – OPTION 2
EVALUATE A SECURITY TOPIC (of your choice)

<table>
<thead>
<tr>
<th>TOPIC AND OUTLINE</th>
<th>Study and evaluate the issues regarding a specific information systems security topic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The following topics are a selection of security areas – these are suggestions only – some of these areas are too broad and should be narrowed to one particular topic area.</td>
</tr>
<tr>
<td></td>
<td>- Individual privacy - IS security implications</td>
</tr>
<tr>
<td></td>
<td>- Current trends in IS security</td>
</tr>
<tr>
<td></td>
<td>- Theories and models for IS security planning</td>
</tr>
<tr>
<td></td>
<td>- Breaches or threats or controls</td>
</tr>
<tr>
<td></td>
<td>- Organisational and managerial security issues</td>
</tr>
<tr>
<td></td>
<td>- Sarbanes Oxley Act</td>
</tr>
<tr>
<td></td>
<td>- Security standard(s) – eg ISO17799</td>
</tr>
<tr>
<td></td>
<td>- Internal system controls including logs and audit controls</td>
</tr>
<tr>
<td></td>
<td>- Security policies</td>
</tr>
</tbody>
</table>

DO NOT UNDER ANY CIRCUMSTANCES PREPARE YOUR TOPIC ON INTERNET SECURITY OR IS SECURITY OR E-COMMERCE-TOO BROAD!

REQUIREMENTS

- The topic should be focused and given an in-depth treatment, not a general overview.
  - This research is to be literature-based.
  - The assignment submission is to be in the form of an academic paper. This includes: an introduction to the topic and an overview of the paper, body of the paper and a conclusion.
  - All externally sourced material must be cited in the body of the paper, and a full description of the source provided in the reference list
  - The main focus of the assignment must be to evaluate the chosen topic, it is not to be a technical paper; therefore including numerous technical descriptions and diagrams will not be marked.

<table>
<thead>
<tr>
<th>WORD LENGTH</th>
<th>approximately 2,500 - 3000 words</th>
</tr>
</thead>
<tbody>
<tr>
<td>REFERENCING</td>
<td>15 references (at least) – no more than 10 references should come from internet sources</td>
</tr>
</tbody>
</table>
|             | The reference list must be placed at the back of the assignment; a reference for this assignment means you have used a source to develop your critique and this source must be cited in the body of the paper as well as correctly referenced in the reference list. (If you are unsure how to display your references, see SIMS Style Guide which is available on the SIMS website.)
|             | **NB: Assignments that lack references in the body, but have a comprehensive reference list will be heavily penalised OR NOT MARKED.** |

NB: If you have a topic that you would like to address that does not appear on the above list, please liaise with your tutor/lecturer as to the suitability of the topic.
MARKING GUIDE

This marking guide should be used to support your assignment – a more stringent and comprehensive marking guide will be followed.

| HD 80-100 | A comprehensive coverage of the topic – answering all the requirements of the assignment  
|           | Excellent essay structure – easy to follow, headings used effectively  
|           | Excellent supporting evidence, clear explanations, descriptions flow logically from one point to the next in a clear and logical sequence  
|           | Higher level considerations  
|           | Sound and useful security enhancements provided supported by evidence  
|           | References correctly cited in body of text and in list – more than 15  
|           | Excellent grammar, spelling, presentation neat and tidy and easy to follow |

| D 70-79 | A very good coverage of the topic with a good level of supporting evidence; and includes reasonably clear explanations,  
|         | logical sequencing from one topic to the next  
|         | Some additional considerations offered  
|         | security enhancements provided, supported by evidence  
|         | Good grammar, minimum spelling errors, presentation neat and tidy and easy to follow  
|         | References used correctly in body and in list (at least 15 cited) |

| C 60-69 | A reasonable coverage of the topic with some level of supporting evidence.  
|         | A fair to moderate level of evaluation and explanation of the topic has been demonstrated but is limited in its scope.  
|         | Sequencing in some logical style but links are inadequate in places  
|         | Some security enhancements offered with supporting evidence but little indepth knowledge displayed.  
|         | Reasonable grammar and some spelling errors, presentation neat and tidy  
|         | Referencing used correctly but some may be missing in the body of the text (less than 15<) |

| P 50-59 | A basic coverage of the topic, with little indepth knowledge demonstrated indicating lack of reading.  
|         | Poor logical sequencing.  
|         | Little or no in depth analysis attempted.  
|         | Headings limited.  
|         | Grammatical and spelling errors – basic presentation  
|         | referencing style incorrect or inappropriate  
|         | References listed do not correspond to those shown in the report (<10). |

| NP <49 | Insufficient coverage of the topic or the topic was one that was not related to information system security.  
|        | No evidence of additional reading to support the argument.  
|        | Absence of any indepth analysis of the topic.  
|        | Overall poorly organised and displayed.  
|        | Less than acceptable grammar and spelling.  
|        | Insufficient and incorrect referencing style |

NB: The topic must clearly reflect IS security.