MONASH University

Faculty of Information Technology

School of Information Management and Systems

IMS5002 – Information Systems Security

MAJOR ASSIGNMENT

Major Assignment	Due Date*	Hand in	% Allocation
Assignment – Part 2	**Week 11 – Friday 21 May**	In IMS5002 assignment box by 5.00 pm	30
TOTAL			30

* See IMS5002 Unit outline regarding assignment extensions (page 6 of 7)

AIMS
The aims of the assignment are to:

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

ASSIGNMENT PRESENTATION

a) A word count must be provided.
b) Assignments that are excessively long or unreasonably short will be penalised.
c) Headings and sub-headings should be used as appropriate.
d) A contents page should be provided.
e) Submissions must be word processed and provided in hard copy by the due date. (See page 6 of Unit outline regarding standards for presentation.)
f) 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)

NB: Please DO NOT provide an abstract or an executive summary.

If you are uncertain as to the approach your assignment should take please discuss the issues with your tutor.

INTRODUCTION

You may choose one of the three assignment options:
Option 1 provides you with a specific topic.
Option 2 allows you to choose from a range of selected topics.
Option 3 is an open topic of your own choosing but this MUST be arranged in advance with your tutor.

Main assignment

Due Date:	Week 11 – Friday 21 May
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)
Allocation	30%
Word count	approximate length 3000 - 3500 words

OPTION 1 – A REPORT

Background

Carl Herberger(2002) *a security expert at SunGard Planning Solutions, discusses the impact of Integrating Business Continuity and Information Security. He states that:*

> 'While information disasters have unlimited potential to destroy corporate productivity, information assets, and reputation, the damage is in many ways quantifiable. According to computer economics, a Carlsbad, California firm that analyses the impact of viruses and other computer security threats, corporations spent more than $12 billion in 2001 cleaning up virus damage. The biggest culprit was the well-publicized code red, estimated to have caused $2.6 billion in damages and infected 300,000 computers. All told, 35 percent of the organizations surveyed in a recent CSI/FBI study reported financial losses, with an average total loss of over $2 million.
>
> These statistics demonstrate the potential for disaster, in terms of a company's ability to conduct business. What they do not show is how the ever-increasing reliance on IT infrastructure significantly compounds the threat. CIOs and IT managers oversee an environment consisting of evolving technologies such as: mobile workforce expansion, the spread of wireless technologies, and the adoption of web services (intranets, internet and extranets) outside traditionally secured data centres making information security a growing and moving target. In addition, although declining in number, there is still a large majority of attacks which originate from insiders.

	The primary challenge organizations face is establishing an holistic framework that addresses information system security and ultimately disaster recovery whilst reflecting stakeholder concerns regarding security. This is not easily done, since information security breaches have some unique and perplexing characteristics, including: damage that may go unnoticed for days or weeks; root causes that can be troublesome to diagnose; symptoms that may recur indefinitely until reparatory action is taken; and damage whose depth and breadth is difficult to assess.' Herberger, C. (2002). Integrating Business Continuity and Information Security (pp 28-32). retrieved on 9 May 2004 located at http://www.contingencyplanning.com/Channels/Security/integratingbusiness.asp
Your brief:	You work for a large organisation which has merged with an organisation that is acknowledged as having a 'loose' security culture. The merger was a strategic move for your organisation. As an outcome of the merger, both the CIO and CSO retired from the merged company without leaving details of the IT and IS security infrastructure. Therefore as Chief Security Officer you have been asked to work together with your Chief Information Officer and IT Manager, to establish an holistic security strategy which needs to be in place by mid to late 2005. 1 ***Describe*** in depth the security strategy you will adopt and provide a timeline within which the strategy will be rolled out within the organisation. To support and enhance your description, you may present this strategy in the form of a diagrammatic representation. 2 As part of your strategy, you should adopt a risk based strategic assessment and planning technique which is specifically designed for IS security. Describe this technique in detail and discuss how it will be used to develop your security initiative. NB: As part of your answer you should include any standards you will adhere to and other issues that should be considered
WORD LENGTH	3000 – 3500 words
REFERENCING	➢ 20 references (at least) – no more than 10 references should come from internet sources ➢ 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 report 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.**

OPTION 2 – Literature review

REQUIREMENTS	• The requirement is to study and review a specific information systems security topic. (See below.) • This research is to be **literature-based.** • The assignment submission is to be in the form of an academic paper. • 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.
TOPICS	❖ Individual privacy - IS security implications ❖ Codes and encryption ❖ Current trends in IS security ❖ Theories and models for IS security planning ❖ A review of IS security research ❖ Breaches, threats, controls, vulnerabilities ❖ Organisational and managerial security issues ❖ Ethical, legal and criminal security issues ❖ Use of security standards ❖ Internal system controls including audit controls ❖ Computer forensics ❖ Security policies and organisational culture ❖ IS security standards NB: The topic must clearly reflect IS security. **DO NOT UNDER ANY CIRCUMSTANCES PREPARE YOUR TOPIC ON:** • **INTERNET SECURITY,** • **IS SECURITY OR** • **E-COMMERCE- THESE ARE TOO BROAD.!** • **SECURITY TOOLS**
WORD LENGTH	3000 – 3500 words
REFERENCING	➢ 20 references (at least) – no more than 10 references should come from internet sources ➢ 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

OPTION 3 - EVALUATION OF AN IS SECURITY TOPIC (of your choice)

REQUIREMENTS	Study and review the issues regarding a specific information systems security topic OF YOUR CHOICE. You must liaise with your tutor as to a suitable topic
TOPIC AREAS	The topic should be given an in-depth treatment, not a general overview. The main focus of the assignment must be a critique and evaluation of the chosen topic, it is not to be a technical paper; ***therefore including numerous technical descriptions and diagrams will not be marked***. **DO NOT DO:** ➢ **internet security** ➢ **e-commerce and IS security** ➢ **IS security** ➢ **Biometrics** ➢ **Specific security tools: firewalls, IDSs, anti-virus etc**
WORD LENGTH	3000 – 3500 words
REFERENCING	➢ 20 references (at least) – no more than 10 references should come from internet sources ➢ 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.

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 Excellent structure – easy to follow, headings used effectively Excellent supporting evidence and critical assessment, clear explanations, flow from one point to the next in logical sequence Higher level considerations Sound and useful future security enhancements provided supported by evidence References correctly cited in body of text and in list – more than 20 References include a variety of sources: journal, texts, whitepapers - not more than 10 references should come from ***APPROPRIATE*** internet sources Excellent grammar, spelling, neat and tidy
D 70-79	A very good coverage of the topic with a good level of supporting evidence; critical assessment evident, reasonably clear explanations, logical sequencing used Some additional considerations offered Future security enhancements provided, supported by evidence References used correctly in body and in list (20 cited) Good grammar, minimum spelling errors, neat and tidy
C 60-69	A reasonable coverage of the topic with some level of supporting evidence. Critical assessment has been demonstrated but is limited in its scope. Fair to moderate explanations. Sequencing in some logical style. Some security enhancements offered with supporting evidence but little indepth knowledge displayed. Referencing used correctly (20<) Reasonable grammar and spelling, neat and tidy
P 50-59	A basic coverage of the topic, all questions answered but little indepth knowledge demonstrated indicating lack of reading. Poor logical sequencing. Little or no critical analysis attempted. Headings limited. Some grammatical and spelling errors – basic presentation Referencing limited or inappropriate reference sources(<20) referencing style incorrect or inappropriate References listed do not correspond to those shown in the report.
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 critical analysis. Poorly organised and displayed. Less than acceptable grammar and spelling. Insufficient and incorrect referencing