IMS3110 INFORMATION SYSTEMS SECURITY

Week 1
Introduction to IMS3110
IS Security introduction and overview
Lecturer: Sue Foster

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.


- SEE UNIT OUTLINE FOR ADDITIONAL REFERENCES

IMS5002 Unit coordinator/lecturer

- Unit Coordinator - Sue Foster
- Lecturer: Sue Foster
  - Email: sue.foster@sim.s.monash.edu.au
  - Office hours by appt

Unit Assessments

- ASSESSMENT ..... 40%
- Assignments
  - 1 – 5% Due date Tutorial 4 - week beginning 15 August
  - 2 – 20% Due date Friday 7 October 5pm – IMS3110 drop box in extreemly urgent and unusual circumstances beyond the control of the student; in this case evidence must be provided
- Tutorial exercise
  - 7.5% Due date Tutorial 11 - week beginning 10 October
- Group presentation
  - 7.5% Group presentations start in Tutorial 3, week beginning 8 August
- FINAL EXAM ..... 60%
In order to pass a unit, a student must gain all of the following:

- 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 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 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’.

**Course Structure – IMS3110**

<table>
<thead>
<tr>
<th>Tutee</th>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>26 September to 30 September</td>
<td>MID SEMESTER BREAK</td>
</tr>
<tr>
<td></td>
<td>5 September</td>
<td>Security design</td>
</tr>
<tr>
<td></td>
<td>8 August</td>
<td>Risk management</td>
</tr>
<tr>
<td></td>
<td>1 August</td>
<td>IS Security – access controls</td>
</tr>
<tr>
<td></td>
<td>24 July</td>
<td>Breaches, threats, vulnerabilities and controls</td>
</tr>
<tr>
<td></td>
<td>18 July</td>
<td>Introduction to IS Security in organisations</td>
</tr>
<tr>
<td></td>
<td>17 October</td>
<td>Privacy, ethics, and the law</td>
</tr>
<tr>
<td></td>
<td>10 October</td>
<td>Business continuity plans (BCP) and disaster recovery</td>
</tr>
<tr>
<td></td>
<td>3 October</td>
<td>Security management - security policies and standards</td>
</tr>
<tr>
<td></td>
<td>19 September</td>
<td>Security design</td>
</tr>
<tr>
<td></td>
<td>12 September</td>
<td>Risk management</td>
</tr>
<tr>
<td></td>
<td>5 September</td>
<td>Internet security</td>
</tr>
<tr>
<td></td>
<td>29 August</td>
<td>E-commerce – Internet security</td>
</tr>
<tr>
<td></td>
<td>22 August</td>
<td>Risk analysis</td>
</tr>
<tr>
<td></td>
<td>15 August</td>
<td>Assignment 1 due</td>
</tr>
<tr>
<td></td>
<td>8 August</td>
<td>IS Security – IS security framework</td>
</tr>
<tr>
<td></td>
<td>1 August</td>
<td>Assignment 2 due</td>
</tr>
<tr>
<td></td>
<td>25 July</td>
<td>Review and Revision</td>
</tr>
<tr>
<td></td>
<td>18 July</td>
<td>Exam Preparation</td>
</tr>
<tr>
<td></td>
<td>10 am – 11 am</td>
<td>F/F 2.12 Thursday Syie Yiing Lum</td>
</tr>
<tr>
<td></td>
<td>11 am – 12 noon</td>
<td>F/F 4.32 Thursday Namit Surana</td>
</tr>
<tr>
<td></td>
<td>12 noon – 1 pm</td>
<td>F/F 3.26 Friday Namit Surana</td>
</tr>
<tr>
<td></td>
<td>12 noon – 1 pm</td>
<td>B/B 4.45 Friday Syie Yiing Lum</td>
</tr>
<tr>
<td></td>
<td>9 am – 10 am</td>
<td>F/F 3.17 Friday Closed off</td>
</tr>
</tbody>
</table>

**Tutorial Allocations**

<table>
<thead>
<tr>
<th>Tutorial</th>
<th>Tutor</th>
<th>Day</th>
<th>Room</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Namit Surana</td>
<td>Thursday 12:00 - 1:00</td>
<td>T1.03</td>
<td><a href="mailto:Namit.Surana@infotech.monash.edu.au">Namit.Surana@infotech.monash.edu.au</a></td>
</tr>
<tr>
<td>3</td>
<td>Namit Surana</td>
<td>Thursday 12:00 - 1:00</td>
<td>T1.03</td>
<td><a href="mailto:Namit.Surana@infotech.monash.edu.au">Namit.Surana@infotech.monash.edu.au</a></td>
</tr>
<tr>
<td>5</td>
<td>Syie Lum</td>
<td>Thursday 12:00 - 1:00</td>
<td>T1.03</td>
<td><a href="mailto:Syie.Lum@infotech.monash.edu.au">Syie.Lum@infotech.monash.edu.au</a></td>
</tr>
<tr>
<td>7</td>
<td>Syie Lum</td>
<td>Thursday 12:00 - 1:00</td>
<td>T1.03</td>
<td><a href="mailto:Syie.Lum@infotech.monash.edu.au">Syie.Lum@infotech.monash.edu.au</a></td>
</tr>
</tbody>
</table>

**Tutorial Topics**

<table>
<thead>
<tr>
<th>Tutorial</th>
<th>Topic</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-2</td>
<td>Review and Revision</td>
<td>15 August</td>
</tr>
<tr>
<td>3-5</td>
<td>Exam Preparation</td>
<td>26 September to 30 September</td>
</tr>
<tr>
<td>6-7</td>
<td>Presentation 1 &amp; 2</td>
<td>8 August</td>
</tr>
<tr>
<td>8-9</td>
<td>Presentation 3</td>
<td>1 August</td>
</tr>
<tr>
<td>10-11</td>
<td>Presentation 4</td>
<td>24 July</td>
</tr>
<tr>
<td>12-13</td>
<td>Presentation 5</td>
<td>18 July</td>
</tr>
<tr>
<td>14-15</td>
<td>Presentation 6</td>
<td>15 August</td>
</tr>
<tr>
<td>16-17</td>
<td>Presentation 7 &amp; 8</td>
<td>29 August</td>
</tr>
<tr>
<td>18-19</td>
<td>Presentation 9 &amp; 10</td>
<td>12 September</td>
</tr>
<tr>
<td>20-21</td>
<td>Presentation 11</td>
<td>5 September</td>
</tr>
<tr>
<td>22-23</td>
<td>Presentation 12</td>
<td>22 August</td>
</tr>
<tr>
<td>24-25</td>
<td>Presentation 13</td>
<td>15 August</td>
</tr>
<tr>
<td>26-27</td>
<td>Presentation 14</td>
<td>8 August</td>
</tr>
<tr>
<td>28-29</td>
<td>Presentation 15</td>
<td>1 August</td>
</tr>
<tr>
<td>30-31</td>
<td>Presentation 16</td>
<td>24 July</td>
</tr>
<tr>
<td>32-33</td>
<td>Presentation 17</td>
<td>18 July</td>
</tr>
<tr>
<td>34-35</td>
<td>Presentation 18</td>
<td>15 August</td>
</tr>
<tr>
<td>36-37</td>
<td>Presentation 19</td>
<td>8 August</td>
</tr>
<tr>
<td>38-39</td>
<td>Presentation 20</td>
<td>1 August</td>
</tr>
<tr>
<td>40-41</td>
<td>Presentation 21</td>
<td>24 July</td>
</tr>
<tr>
<td>42-43</td>
<td>Presentation 22</td>
<td>18 July</td>
</tr>
<tr>
<td>44-45</td>
<td>Presentation 23</td>
<td>15 August</td>
</tr>
<tr>
<td>46-47</td>
<td>Presentation 24</td>
<td>8 August</td>
</tr>
<tr>
<td>48-49</td>
<td>Presentation 25</td>
<td>1 August</td>
</tr>
<tr>
<td>50-51</td>
<td>Presentation 26</td>
<td>24 July</td>
</tr>
<tr>
<td>52-53</td>
<td>Presentation 27</td>
<td>18 July</td>
</tr>
<tr>
<td>54-55</td>
<td>Presentation 28</td>
<td>15 August</td>
</tr>
<tr>
<td>56-57</td>
<td>Presentation 29</td>
<td>8 August</td>
</tr>
<tr>
<td>58-59</td>
<td>Presentation 30</td>
<td>1 August</td>
</tr>
<tr>
<td>60-61</td>
<td>Presentation 31</td>
<td>24 July</td>
</tr>
<tr>
<td>62-63</td>
<td>Presentation 32</td>
<td>18 July</td>
</tr>
<tr>
<td>64-65</td>
<td>Presentation 33</td>
<td>15 August</td>
</tr>
<tr>
<td>66-67</td>
<td>Presentation 34</td>
<td>8 August</td>
</tr>
<tr>
<td>68-69</td>
<td>Presentation 35</td>
<td>1 August</td>
</tr>
</tbody>
</table>

**Contact Information**

Phone: 9903 2631
Email: Namit.Surana@infotech.monash.edu.au
Room: T1.03
Tutorial Expectations

- Students are to confine themselves to the tutorial they are allocated to
- Students should provide their full names with correct spelling at their first tutorial
- Some tutorials are full – do not worry!!
  - attend the one you would normally allocate to
  - we will evaluate this situation in Week 3

Lecture Objectives

- Describe IS Security
- Understand the need by organisations for information system security
- Describe the issues which influence IS Security in organisations
- Describe the basic characteristics of an information systems security

What Is Security

Security is defined as the policies, practices and technology that must be in place for an organisation to transact business electronically via networks with a reasonable assurance of safety

(Volonne & Robinson, 2004)

**IS THIS DEFINITION SUFFICIENTLY INDEPTH??**

Why Do We Need Security

To Protect a Company’s Assets

- From
  - Corporate espionage
  - Sabotage
  - Disgruntled employees
  - Hackers
  - Fraudulent activities (remove temptation)
  - Terrorists
  - Accidental incidents
Visa, Amex cut ties with processing firm hit by security breach

After October, CardSystems won't be allowed to process their transactions. (July 20, 2005)

Visa and American Express Co. are terminating their contracts with a credit card transaction processing company that was hit by hacker attacks, potentially exposing 40 million card numbers to online intruders.

Security breach may have exposed 40M credit cards

Security firm details six unpatched Oracle flaws

The German company said it warned Oracle about them two years ago.

Oracle moves to quarterly patch release schedule

Users want a more predictable process for applying security fixes

Security breach may have exposed 40M credit cards

Security firm details six unpatched Oracle flaws

The German company said it warned Oracle about them two years ago.

Oracle moves to quarterly patch release schedule

Users want a more predictable process for applying security fixes

Visa, Amex cut ties with processing firm hit by security breach

After October, CardSystems won't be allowed to process their transactions.

Visa and American Express Co. are terminating their contracts with a credit card transaction processing company that was hit by hacker attacks, potentially exposing 40 million card numbers to online intruders.

Security breach may have exposed 40M credit cards

Security firm details six unpatched Oracle flaws

The German company said it warned Oracle about them two years ago.

Oracle moves to quarterly patch release schedule

Users want a more predictable process for applying security fixes

Security breach may have exposed 40M credit cards

Security firm details six unpatched Oracle flaws

The German company said it warned Oracle about them two years ago.

Oracle moves to quarterly patch release schedule

Users want a more predictable process for applying security fixes

Related to this topic

- Breach of Credit Data May Have Broad Scope>
- Laptop with credit card info for 80,000 DOJ workers stolen>
- Visa USA adds tool to its credit card antifraud arsenal>
- Blog: Remember when people thought e-commerce was ‘risky’?
- Microsoft tweaks certification programs

http://www.computerworld.com/databasetopics/data/story/0,10801,102631,00.html
Security issues!!

Simon Vallor a 22 year old Welsh Web designer and hacker, was tracked down by the FBI and Scotland Yard after creating one of the world’s most widespread viruses.

He pleaded guilty under the Computer Misuse Act and was sentenced in January 2003 to two years in jail, one of the heaviest sentences yet for spreading computer viruses.

Vallor was caught because he boasted in an Internet chat room under the name “Gobo” that “at last there’s a WELSH VIRUS”


Nigeria Jails Woman In $242M E-mail Fraud Case

A Nigerian court has sentenced Amaka Anajemba to two and a half years in jail for her role in the country’s biggest e-mail scam case, the Economic and Financial Crimes Commission said.

http://www.computerworld.com/newsletter/0,4902,103307,00.html?nlid=SEC

What does all this mean?

Security From Within And Without

- SECURITY SHOULD NOT JUST BE ABOUT KEEPING INTRUDERS OUT BUT
- LIMITING AND REPAIRING THE DAMAGE WHEN THEY GET IN
  - SPEED
  - Intrusion detection
  - BCP and Disaster recovery planning
  - BE PREPARED
  - CIA Model
A secure information system is designed to protect information resources:

- HARDWARE
- SOFTWARE
- DATA
- COMMUNICATION NETWORKS
- ANY PHYSICAL FACILITIES USED IN THE TRANSMISSION, PROCESSING AND STORAGE OF INFORMATION

In the 80s and 90s increased threats and breaches due to:
- Growing computer literacy
- Greater availability of low-cost computer technology
- Widespread usage and access
- Total dependency on systems; "denial of service" threat
- "hostile" and "open" environments
- Emerging new technology
- Growth of the internet

IS Security Objective: protect information resources, by maintaining security goals:
- Confidentiality (secrecy)
- Integrity
- Availability

A security analyst analyses a system’s security to comply with the CIA model

Security Threats impacting on CIA goals
- Availability
  - Denial of Service
  - Sabotage

- Data Integrity/ Authenticity
  - Data Tampering

- Confidentiality/privacy
  - Sniffing
  - Eavesdropping
  - Theft
  - Espionage
  - Identity theft
  - Financial fraud
Security Depends on People

From Information Security Magazine - “What is the top obstacle? What do you consider is the SINGLE greatest obstacle to achieving adequate infosecurity at your organization?”

Security must be a conscious priority.

WHAT ARE THE ISSUES FACING AN ORGANISATION FROM POOR IS SECURITY?

- Budget constraints
- Lack of Security Management Support
- Lack of Competent Information Security Personnel
- Lack of Awareness
- Lack of Control
- Lack of Authorization
- Technical Complexity
- Other

The Cost of Computer Crime

The following table shows the average cost of computer crimes and security breaches over a 12-month period.

<table>
<thead>
<tr>
<th>Type of Breach</th>
<th>Total Cost ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized Access</td>
<td>40,000</td>
</tr>
<tr>
<td>Software Defects</td>
<td>30,000</td>
</tr>
<tr>
<td>Data Recovery</td>
<td>20,000</td>
</tr>
<tr>
<td>Malware</td>
<td>15,000</td>
</tr>
<tr>
<td>Identity theft</td>
<td>10,000</td>
</tr>
<tr>
<td>Phishing</td>
<td>5,000</td>
</tr>
<tr>
<td>Total Cost</td>
<td>100,000</td>
</tr>
</tbody>
</table>

Technology, Process, People

What are the challenges?

- Products lack security features
- Products have bugs
- Many issues are not addressed by technical standards
- Too hard to stay up-to-date

- Design for security
- Roles & responsibilities
- Audit trails, computer forensics, follow-up
- Disaster recovery plans
- Stay up-to-date with security development
Security management

- Management commitment to IS security
  - CIO/CEO
  - Budget
  - Insourcing/Outsourcing of security
    - Does it suit your organisational requirements
  - Risk Management
    - http://www.cert.org/octave/omig.html
- Organisational wide Security philosophy
- Security Champion –
  - Chief Security Officer (CSO)
- Security Policy and procedures

Consider Security for different IS architectures

- Map security architecture
  - Security framework
  - Business processes
    - (gap analysis)
- Legacy systems
- Open distributed systems
- Wireless
- Mobile

Common Security Safeguards

- Password protection (password management)
- Intrusion Detection Systems (IDS)
- Virus prevention software
- Public Key Infrastructure - Cryptography
  - Digital Certificates
- Firewalls
- SSL (secure socket layer)
- Security Monitors, surveillance techniques

Common Security Sites

- CHECK COMMON SECURITY SITES:
  - SANS (SYSTEM ADMINISTRATON, NETWORKING AND SECURITY INSTITUTE)
    - www.netiq.com
  - CERT (COMPUTER EMERGENCY RESPONSE TEAM)
    - Offer warnings announcements and updates
      - http://www.cert.org/
  - MANY OTHERS
**REVIEW QUESTIONS**

- Discuss reasons why threats to computer systems have been increasing through the 1980s and 1990s.
  - Do you think this trend will continue?
  - Give reasons for your answer
- Why is information security management important?

**IMPORTANT WEBSITES**

  Some interesting current federal US court cases on security breaches:
- [http://www.isaca.org/Template.cfm?Section=About_Isaca&Template=/ContentManagement/ContentDisplay.cfm&ContentID=9755#saranes](http://www.isaca.org/Template.cfm?Section=About_Isaca&Template=/ContentManagement/ContentDisplay.cfm&ContentID=9755#saranes)

**Articles**