TOPIC: Designing a secure information system

Learning outcomes:
• Adopt a holistic approach to information system security
• Identify the most important security measures that should be used to secure an information system
• Describe the security measures you identify to reflect a “defence in depth strategy”
• Use case study information to develop a suitable and informative answer to the brief provided.

<table>
<thead>
<tr>
<th>TIME FRAME</th>
<th>TOPIC</th>
<th>ACTIVITY</th>
<th>OUTCOMES/RESOURCES etc</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 mins</td>
<td>Real world IS Security case</td>
<td>The following question was taken from the IMS5002 final exam paper in 2004. Please read question 3 and develop the following brief. Your Brief: As the new Chief Security Officer for this organisation (the other CSO was fired), in the form of a diagram develop the effective security measures you would implement to reduce the chances and impacts of this and other such breaches occurring in the future. Your tutor will develop this further when you have completed the activity.</td>
<td>Use the defence in depth diagram over the page to help you develop your answer. Use the discussion points to develop a holistic approach to system security. To help you with this exercise access the following website to read some of the relevant articles: <a href="http://www.cert.org/nav/articles_reports.html">http://www.cert.org/nav/articles_reports.html</a></td>
</tr>
<tr>
<td>15 mins</td>
<td>Presentations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Question 3: Taken from IMS5002 Exam paper 2004. Real World IS Security Case

In a recent case, an Australian organisation’s publicly accessible payroll system was broken into by exploiting a known operating system level vulnerability. The company had not enabled logging at the network, database or operating system levels, providing investigators with virtually no forensic trail.

Investigations showed that the administrator’s desktop computer was similarly compromised. This provided the investigating team with some evidence that the payroll system may have been the target of a deliberate, rather than random attack. It also suggested that the attack was most likely perpetrated by an employee, or someone who would have knowledge of the system and who could benefit from modifying the data within it. However, without adequate logging it was difficult to mount a thorough investigation, let alone prove a case. As with any major compromise of a mission critical system, recovery was painful and protracted (p28).

DISCUSSION POINTS:

- Is anything missing from this diagram
- Is this diagram sufficient to create a defence in depth strategy?