## TOPIC: RISK MANAGEMENT – security risks in e-commerce

**Learning outcomes:**
- Describe the main risks organisations are faced with when implementing an e-commerce strategy.
- Identify the main types of security controls that would be advisable to use to protect critical assets.
- Using a business case, describe a security strategy together with the controls that could be used.
- Identify the importance of non-repudiation in the use of e-commerce.

<table>
<thead>
<tr>
<th>Time frame</th>
<th>Topic</th>
<th>Activity</th>
<th>Outcomes/tasks/resources</th>
</tr>
</thead>
</table>
| 10 minutes | e-commerce – the risks | General Group discussion:  
- What are the main risks to organisations conducting e-commerce?  
- What main types of security controls would you put in place to support an e-commerce initiative? | |
| 25 mins | Presenting findings | GROUP DISCUSSION:  
You are considering opening a video store. As part of your strategic business initiative you are going to offer customers online access to your videos so they can purchase/rent on line.  
- This is going to present numerous security problems.  
- In groups describe in diagrammatic format the security strategy you would implement, including the types of security controls you would put in place to protect your information systems.  
- What procedures would you put in place to ensure non repudiation. Put this on your diagram.  
- You will need to justify your choice of security controls to your tutor.  
CLASS DISCUSSION:  
- Your tutor will develop the diagrams from the different group.  
- Students from different groups will be asked to place their security controls strategically on the diagram on the whiteboard.  
- You will have to provide reasons for your choice of specific security controls. This should reflect a “defence in depth” strategy.  
Please access the following websites ready for your tutorial.  
Summary of the top 10 internet security tips. Australian Government located at:  
E-business guide: a guide to doing business online (2004). Australian Government located at:  
Develop a “defence in depth approach” to security. | |
| 15 mins | Presentation | | |
| 10 mins | Assignment 1 feedback | Assignments will be given back and will include a marking guide | If you need to discuss in detail the marking please see your tutor during their consultation time.
Four types:

- **Deterrent controls**
  - reduce the likelihood of a deliberate attack
  - Example?

- **Preventative controls**
  - protect vulnerabilities and make an attack unsuccessful or reduce its impact
  - Example

- **Corrective controls**
  - reduce the effect of an attack
  - Example

- **Detective controls**
  - discover attacks and trigger preventative or corrective controls
  - Example
DEFENCE IN DEPTH APPROACH TO INFORMATION SYSTEM SECURITY

DEFENCE IN DEPTH – PRIMARY AREAS

- Risk management
  - OCTAVE/CRAMM/COBRA
- Perimeter defences
  - Routers
  - Firewalls
- Access controls
- Network defences
  - IDS (intrusion detection systems)
- Encryption
- Policy definition and management
- Physical defences
- Virus detection
- Application protection
  - Vulnerability scanning