Course Outline and Structure

- Week 1: Security Governance
- Week 2: Managing Security in the organisation
- Week 3: Risk Management
- Week 4: IS Security
- Week 5: Computer forensics
- Week 6: The role of security
- Week 7: The impact of e-commerce on the organisation
- Week 8: The role of e-security
- Week 9: Risk Management Part 4
- Week 10: Business continuity plans
- Week 11: Security standards, Privacy and law
- Week 12: Current issues and future trends
- Week 13: Revision and exam preparation

Agenda:

Introduction
- What is a security policy?
- Who should invest in Security Policies?

Four Pillars of Security
1. Build a security framework
2. Identify critical weaknesses and risks
3. Corporate 'policies' and 'standards'
4. Monitoring and Reviewing

Benefits

Links

Questions

Aim: There must be a comprehensive, unified approach to security.

No half measures.

The Problem

Within today’s organisation they must be prepared and flexible enough to combat multiple threats to their environment.

What can an organisation do to protect themselves from these multiple threats? Where do people go when they want to identify the company’s strategy to mitigate these risks?

The following are common threats impacting the modern day organisation:

1. Viruses
2. Hacking
3. Reporting Security Weaknesses
4. Internet Commerce threats
5. Fires, Floods, Earthquakes
6. User making errors
7. Users committing crimes via the Internet

Of 643 Surveyed 90% detected security attacks

Remember: Be aware of the threats! Yes – it can happen to you.
The Problem?

Internet attacks are on the rise
- Attack level of sophistication is on the rise
- Ease of use is increasing – L0pht Crack
- Software now exists that allow novices to run complex attacks – Script Kiddies

How does an ‘organisation’ know what they must do to identify these threats, and what controls are needed once they have done so?

Remember: Script Kiddies will bite more than your ankles….

The Answer….

Security Policies

Security Policies – The Rational

Some of the requirements and rationales behind why policies should be adopted:

1. Policies are supported by executive management.
   - Rationale: Executive management support forms part of a top-down security approach. Management support gives the new security system credibility among employees. This increases buy-in of the new security system, facilitating successful implementation and enforcement.

2. Policies are statements of management intent.
   - Rationale: This imbues the policies with properties of authority and legitimacy. Management intent suggests to employees that policies are intended to be binding and followed in all corporate activities ranging from creating or modifying standards, to employee day-to-day tasks.

3. Policies must be justifiable in the eyes of staff and management.
   - Rationale: Staff and management must find the policy acceptable. This is why it is important to justify each policy.

4. Policies may be traced to one or many business requirements.
   - Rationale: Policy creation or modification may be driven by business needs following proper planning and risk assessment.

5. Policies may be traced to one or many security requirements.
   - Rationale: Ensuring policies comply with security requirements reduces the risk of business operation failure.

No Security Policies?? The Consequences

Some of the requirements and rationales behind why policies should be adopted:

1. No centralised approach to security:
   - Rationale: The security policies provide the organisation with a centrally managed and executive supported approach to information security. By having clear and understandable security policies allow each individual within the organisation to understand their roles and responsibilities as they pertain to information security.

2. Not knowing what a security incident is:
   - Rationale: By not having well defined security policies on incident handling, there is a potential for security breaches and incidents to go unreported. If users are not aware of their responsibilities to report these issues it may put the organisation in a very vulnerable position.

3. No formalised way of reprimand:
   - Rationale: No policies suggest someone downloading pornography or mp3s. What happens if a user has limited grounds to stand on for dismissal?

Why aren’t we all doing it?

1. Time Consuming
   - Rationale: The process of identifying risk can be time consuming. It involves gathering information, analyzing the data and then selecting the appropriate controls.

2. Difficult to do
   - Rationale: Multiple skill sets needed
   - Rationale: Continuous process – Security is ever evolving

3. Management do not see a direct benefit
   - Rationale: Executive management support forms part of a top-down security approach.

4. Deals with multiple levels of the business
   - Rationale: Security policies involve multiple levels of the business.
A Security Policy does NOT include?

• Does not state exactly what hardware and software architecture, protocols will be used to ensure security
  – It does NOT state how the HW and SW will be installed and configured
• Because these details will change from time to time they should be shared only with authorized network administrators or managers (not with all employees).
• Policies are not detailed instructions – Policies are usually endorsed by executive management and signed off by the CIO or CEO. You do not want to be changing policies every few months because a procedure has changed.
• Security Policies – Generally are not measurable

Which companies should develop a security policy? Who will use the security policies?

Ø Organisations that are security aware
Ø Electronic commerce over the Internet
Ø Government organisations automating forms processing
Ø External exposure of data processing environments
Ø Organisations who must be compliant to regulatory boards e.g. APRA, SOX, Aus Energy Board
• IN EFFECT ALL ORGANISATIONS!!
• Management
• Users; Technical Staff; Security Staff
• Contractors
• Outsourcers
• IN EFFECT ALL STAFF!!

Four Pillars to Develop the Security Policy Framework

1. Build a security framework that fits with business requirements
2. Identify critical weaknesses and risks, and remediate key problems
3. Embody security requirements within corporate ‘principles’, ‘policies’ and ‘standards’
4. Monitor the newly formed environment and make changes where appropriate.

Pillar #1: Security Policy Framework

Information security investment is pointless without an effective framework.

The Security Framework is a comprehensive description of the people, processes, and technology components that comprise a complete security capability. The security areas can be used to facilitate security planning and policy design activities. The framework is also valuable as an ‘umbrella’ covering both technical and non-technical security components.

Framework best practice – ISO 17799, COBIT

With the emergence of new technology strategies such as Intranets and Extranets, protection of informational assets has become paramount. The first step is an enterprise-wide Information Systems Security Policy by Rahaju Pal / Dhawal Thakker

The building blocks

Remember: A strong organisation has a strong frame!
Pillar #3: Putting Effective Security Policies in Place

- The ISO 17799 methodology – PDCA (Development of an ISMS)
- High level statements based on management intent
- Policies should be derived from business and security requirements
- Elements within the integrated security architecture should reflect policy requirements
- Based on best practice – ISO 17799, COBIT
- Information security investment is pointless without an effective policy.

Security Principles – And The Answer Is……..

- High level strategic statements on security
  - The principles that the organisation will build their security approach on.
  - All policies, standards, process and procedures must be compliant to the principles
  - Provides the essence of the security framework
  - Usually authorised by the CED/CIO
- Multiple sources of information:
  - Organisation for Economic Co-Operation and Development (OECD)
  - In house principles
- Example:
  - Client: Monash University
  - Security guiding principle:……..

Example: People Risks

- Inadequate using Social engineering or eavesdropping to obtain passwords.
- Admin incorrectly configures user lists, groups, and their associated rights on a file server.
- Network administrators overlook flaws in topology.
- Lack of communication of security policy leading to inadvertent misuse of files.
- Dishonest or disgruntled employees abusing their access rights.
- Unused computer left logged in
- Easy to guess Passwords
- Unlocked doors to computer rooms.
- Discs being discarded in trashcan

<table>
<thead>
<tr>
<th>Potential Risk</th>
<th>Inherent Risk</th>
<th>Known Issues</th>
<th>Audit Regularity</th>
<th>Known Data</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Engineering</td>
<td>High</td>
<td>E</td>
<td>D</td>
<td>C</td>
<td>B</td>
</tr>
<tr>
<td>User Fraud</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Error</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>L</td>
<td></td>
</tr>
<tr>
<td>Social Engineering</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Unattended Equipment</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Network administrators overlook flaws in OS topology.</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Network administrators overlook flaws in OS topology.</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>L</td>
<td>HH</td>
</tr>
<tr>
<td>Dishonest or disgruntled employees abusing their access rights.</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Unused computer left logged in</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Easy to guess Passwords</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Unlocked doors to computer rooms.</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Discs being discarded in trashcan</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>L</td>
<td>H</td>
</tr>
</tbody>
</table>

Understanding risks allow for greater effectiveness of the policies

If the only tool you have is a hammer, you tend to see every problem as a nail.
Security Principles – A Guiding Principle Example

- To ensure that there are controls in place to protect the confidentiality, integrity and availability of all assets within Monash University.

- Security principles are based on what we have already discussed:
  - Other examples:
    - Timeliness
    - Accountability
    - Ethics
    - Non-Reputation

Security Policies – What is wrong with this?

The language in each policy must be clear and must have only one interpretation.

- Rationale: Policies should not be ambiguous and should be interpreted in the way the creator or modifier of the policy intended. This is required for:
  - Effectiveness: This reduces the risk of conflict and confusion which could potentially lead to the creation of non-compliant or inconsistent standards.
  - Efficiency: Resources are used in resolving conflict.
  - Legal Exposure: If disciplinary actions are taken against employees, they may argue that the policies were unclear or ambiguous.

Policy 101 – Password Policy

- Control Objective: To try and protect passwords

Policy Statement:

- Control Objective: To try and protect passwords

Security Policies – A Password Policy Example

- Policy Statement:

  - Control Objective: To control access to Monash University’s assets by providing a set of rules and procedures governing User passwords that must be strictly adhered to.
  - Users must follow ‘Standard 001 – Password use’ in the selection and use of passwords. Passwords provide the principal means of validating a user’s authority to access a computer service. To ensure that the confidentiality of all data and assets within Monash University is protected, strong passwords must be selected.
  - Security Staff: It is a mandatory requirement that all systems are configured to utilise a strong password management system.

Security Standard

- A security standard is:

  - A precise criterion that defines
    - Requirements
    - Rules,
    - Controls or Practices

To ensure Information Security is implemented in accordance with the intent of Information Security Policies. Standards must be measurable, can be technology specific but should not be product specific.

Multiple sources of information:

1. ISO 17799
2. ISO 13335
3. Standards for Good Information Security Practice
4. NIST

Example:

Client: Monash University - Password Standard

Security Standards – And The Answer Is……..
Security Standards – A Password Standard Example

- Standard Statement: In accordance with Policy 101 – Password policy the following requirements must be adhered to when selecting a password. Failure to follow these requirements may be grounds for disciplinary action.
  - All users will select passwords based on the following criteria:
    - Minimum 6 characters
    - Alpha/numeric
    - Changed every 3 months
    - No words from a dictionary
    - No words made up from multiple dictionary words
    - ... A good start what else?

Pillar #4: Monitoring and Improving

- Not all organisations get it right at the start
- Implement the identified improvements in the Security Policy System
- Take appropriate corrective and preventive actions. Apply the lessons learnt from the security experiences of other organisations and those of the organisation itself
- Communicate the results and actions and agree with all interested parties
- Ensure that the improvements achieve the intended objectives
- Record actions and events that could have an impact on the effectiveness or performance
- Apply the lessons learnt from the security experiences of other organisations
- Execute monitoring procedures to:
  - Analyse and process the results of monitoring promptly
  - Identify failed and successful security breaches and incidents promptly
  - Enable management to determine whether the security is performing as expected
  - Review all incidents to prevent similar incidents of security affecting business processes
- Undertake a management review on a regular basis (at least once a year) to ensure that the scope remains adequate and improvements in the process are identified

But is it worth it?

Security: The benefits

Costs
- Development and implementation Costs
- Development of security policies, Purchasing of security policy software
- Software and Hardware Costs
- Buying the infrastructure to leverage the security benefits, Use of risk analysis tools and software
- Professional Services
- Compliance costs – auditors, consultants

Benefits
- Reduction of IT resources as there are stronger and tighter controls in place
- Improved productivity by having clear processes which support business activities
- Example: Well defined and clear processes and controls allow for work to be completed more efficiently
- Reduced Security Incidents
- Reduction of costly security incidents by keeping a closer handle on removal of ghost accounts, accurate enforcement of password policy, etc.
- Increased Opportunities
- Improvement of employees’ or business partners’ contribution to the organization’s bottom line because of the ability to quickly and securely access the company’s infrastructure

Cost Savings
- Reduction of IT resources as there are stronger and tighter controls in place
- Example: Individuals having access revoked after they have left the company – Save money through licensing

... costs vs benefits

Is it worth it? I believe so....

Contacts and Resources

Links:
- www.isaca.org
- www.osbi.org
- www.accenture.com
- www.gsa.gov
- www.securityfocus.com
- www.ffiec.gov/ffiecinfobase/index.html
- http://www.gsa.gov/resources/policies/
- http://www.sans.org/rr/whitepapers/policyissues/

Questions?