Managing Security in the organisation

Step 2: Risk Mitigation – access controls cont/d - authentication

Lecturer: Sue Foster

Week 5

Weekly IS Security topics

<table>
<thead>
<tr>
<th>Date (week beginning)</th>
<th>Weekly IS Security topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 August</td>
<td>Risk Management: Step 2: Risk Mitigation - access controls</td>
</tr>
<tr>
<td>12 September</td>
<td>Risk Management: Step 3: Security policies and procedures</td>
</tr>
<tr>
<td>19 September</td>
<td>Risk Management: Step 4: Internet security cont/d</td>
</tr>
<tr>
<td>22 August</td>
<td>Risk Management: Step 5: Security design</td>
</tr>
<tr>
<td>25 July</td>
<td>Risk Management: Step 6: Security policies etc</td>
</tr>
<tr>
<td>29 August</td>
<td>Risk Management: Step 7: Breaches, Threats, Vulnerabilities</td>
</tr>
</tbody>
</table>

Learning Objectives

- Link IS security goals to protecting vulnerabilities and access controls
- Identify access controls by what they do and how access controls support information system protection
- Understand the importance of a defence in depth approach to information system security

External threats: Trophy Hunting

Symantec and McAfee are targeted by intruders due to the inherent value in breaking into their websites.

3000 to 4000 people each day try to breaking into Symantec website. Most of it is trophy hunting by the intruder

Internal Threats: Employee Revenge

- Defence contractor Lockheed Martin’s email system crashed for six hours after an employee sent 60,000 co-workers a personal email message containing a confirmation request.
- Lockheed which posts 40 million emails each month, was forced to fly in a Microsoft rescue squad to repair the damage
Holistic approach to IS security

Risk analysis/assessment
• Determine critical assets
• Analyse threats
• Statistics
• Current/future trends
• Establish vulnerabilities
• Perform gap analysis

Risk mitigation
Cramm/octave/Cobra
ALE (quant)
Assess current
Access controls
New access controls

Security Framework – goals of IS security
Confidentiality
Availability
Integrity
Authentication
Non-repudiation
Accountability

RISK MANAGEMENT

Security Controls

PROVIDE:
• Protection for vulnerabilities
• Countermeasures against access breaches

Controls

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
• Corrective controls
  - reduce the effect of an attack
• Detective controls
  - discover attacks and trigger preventative or corrective controls


Control Relational Model

THREAT

Corrective Control

Detective Control

Reduced Likelihood of

Deliberate Attack

Vulnerability

Preventative Control

Detected

Prevented

Reduced Impact

Decreases
The Core Issues

- Threats
- Breaches
- Information system
- Controls
- Vulnerabilities

Most Common Inadequate Controls
- Lack of management commitment
- Poorly trained or overworked IT staff
  - Slow system vulnerability awareness to patch time
- Ineffective information security infrastructure
  - Lack of defense in depth
- Inadequate security training or awareness
- Ineffective personnel procedures
- Ineffective risk management
- Insecure document control etc

What Else Can You Do??

Put in place sophisticated Security Controls
- Intrusion detection systems
- Firewalls
- Anti-virus software - updates
- Vulnerability Scanning and analysis tools
  - Provide automatic patching and updates
- Security policies and procedures
- Security logs = audits

Defence In Depth solution – A Layered Strategy

- Physical defence
- Network defence
- Application protection
- Encryption
- Policy definition and management
- Risk management
- OCTAVE/CRAMM/COBRA

Conclusion

The access controls are only as good as the people who support them. IT staff need to be skilled in all facets of access controls from vulnerability management to reviewing a breach.

References

- http://www.thinkmobile.com/News/00/48/29/
- http://www.sophos.com/avleans/whitpapers/abc.html#top
Additional readings:


Revision Questions

- Why is there a need for security systems
- Why develop a defence in depth
- If you were an IT security specialist what would be your most important concerns regarding information system security?

Appendix

http://www.sans.org/newsl etters/

- The Critical Vulnerability Analysis and the Security Alert Consensus have merged to become @RISK: The Consensus Security Alert.
- Delivered every Monday morning, @RISK first summarizes the three to eight vulnerabilities that matter most, tells what damage they do and how to protect yourself from them

More Vulnerabilities:

- Please look at this power point slide: http://www.sans.org/top20/top20paller03.pdf