# Risk Assesment

# Risk Assesment

- What is a Risk
  - It is the likelihood of loss
  - The business is going to loose money
  - Example?
  - Identify a list of possible risks for a web server?
  - Identify a list of possible risks for a campus area network?

# Definition in the context of security

- “The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.”

# Risk Assessment

- Requirement
  - The most important that you understand the business.
  - If the business is using an Antivirus software. What is the reason for this.
  - You need to understand the technical solutions and business side of the risks.

# Risk Assessment

- Risk is a business concept.
- What are the chances that the system will cost the business.
- Loss can come from a number of different sides
- For example web server down time..Will cost money.

# Risk Assessment

- Legal Requirements as well
- If personal information is compromised the business might get sued.
- Data protection Act..
- Management of Health and Safety at Work Regulations

# Regulation 3(1) of the 'Management of Health and Safety at Work Regulations 1992 states:-

- *'Every Employer shall make a suitable and efficient assessment of:-*

  *a) The risks to the health and safety of his employees to which they are exposed whilst they are at work.*

  *b) The risks to the health and safety of persons not in his employment arising out of or in connection with the conduct by him or his undertaking;*

- *For the purpose of identifying the measures he needs to take to comply with the requirements and prohibitions imposed on him by or under the relevant statutory provisions.'*

# How to Calculate

- Example 1.
- Risk= Threat * vulnerability
- Threat : Hacker
- vulnerability : no antivirus
- Risk : High

# How to Calculate

- Example 2.
- Risk= Threat * vulnerability
- Threat : Hacker
- vulnerability : Antivirus, Firewall and strong encryption in place
- Risk : Low

# How to Calculate

- Generally Speaking
  - Risk= Likelihood * Impact
- IT Risk
  - Risk= Threat * vulnerability
- More Recent
  - Risk= Threat * vulnerability *Asset
  - Risk= ((Threat * vulnerability)/CounterMeasure)*AssetValueAtRisk

# How can business loss money

- Hackers
- Downtime
- Legislation
- Lack of Procedures

# Threats

- The forces that can compromise the system
- Examples?

# Vulnurabilities

- What protection you have set up
- For example :
- For Natural disaster what protection you have setup.
- Buy high quality hardware for the setup.

# Risk Management

Risk management can be defined as:

*The eradication or minimisation of the adverse affects of risks to which an organisation is exposed.*

# Risk Management

- Goal
  - Protect the organization’s ability to perform its

    mission (not just its IT assets)
  - An essential management function (not just an IT technical function)

# Risk Assessment Methodology

- Step 1: System Characterization
  - Input:
    - system-related info including
    - Hardware
    - Software
    - System interfaces
    - Data and information
    - People
    - System mission
  - Output:
    - A good picture of system boundary, functions,
    - criticality and sensitivity

# Risk Assessment Methodology

Step 2: Threat Identification

- Input:
  - Threat Sources
    - natural,
    - human,
    - Environmental
  - Motivation and threat Analysis
    - Security violation reports
    - Incident reports
    - Data from intelligence agencies and mass media
- Output:
  - Threat statement listing potential threat-sources applicable to the system being evaluated

# Risk Assessment Methodology

Step 3: Vulnerability Identification

- Input:
  - Vulnerability sources
    - Vulnerability lists/advisories
    - Vendor advisories
    - Audit results etc.
  - System security tests
    - Automated vulnerability scanning tool
    - penetration tests etc.
  - Development of Security requirements checklist (contains basic security standards)
    - Management, Operational, Technical
- Output:
  - List of system vulnerabilities (flaws or weaknesses) that could be exploited –
  - Vulnerability/Threat pairs

# Risk Assessment: Methodology

Step 4: Control Analysis

- Input:
  - Control Methods – may be technical or non-technical
  - Control Categories – preventative or detective (e.g. audit trails
  - Control Analysis
    - Development or use of checklist to analyse controls
- Output:
  - List of current and planned controls

# Risk Assessment: Methodology

Step 5: Likelihood Determination

- Input:
  - Threat-source motivation & capability
  - Nature of the vulnerability
  - Existence & effectiveness of current controls
- Output:
  - Likelihood rating of High, Medium or Low

# Risk Assessment: Methodology

Step 6: Impact Analysis

- Input:
  - System mission
  - System and data criticality
  - System and data sensitivity
  - Analysis:
  - Adverse impact described in terms of loss or degradation of
    - integrity, confidentiality, availability
- Output:
  - Impact Rating of High, Medium or Low

# Risk Assessment: Methodology

Step 7: Risk Determination

- Input:
  - Likelihood of threat
  - Magnitude of risk
  - Adequacy of planned or current controls
- Output:
  - Risk Level Matrix (Risk Level = Threat Likelihood x Threat Impact)
  - Risk Scale and Necessary Actions

# Risk Scale & Necessary Actions

- Risk Level Risk and Necessary Actions
- High
  - Strong need for corrective measures
  - Corrective action plan must be put in place as soon as possible
- Medium
  - Corrective actions are needed
  - Plan must be developed within a reasonable period of time
- Low
  - Determine whether corrective actions are still required or decide to accept the risk

# Risk Assessment: Methodology

Step 8: Control Recommendations

- Input
  - Effectiveness of recommended options
  - Legislation and regulation
  - Organizational policy
  - Operational impact
  - Safety and reliability
- Output:
  - Recommended controls and alternative solutions to mitigate risk

# Risk Assessment: Methodology

- Step 9: Results Documentation
- Output:
  - Risk Assessment Report
  - Presented to senior management and mission owners
  - Describes threats & vulnerabilities, measures risk and provides recommendations on controls to implement
- Purpose:
  - Assist decision-makers in making decisions on policy, procedural, budget and system operational and management changes

- Q & A Session