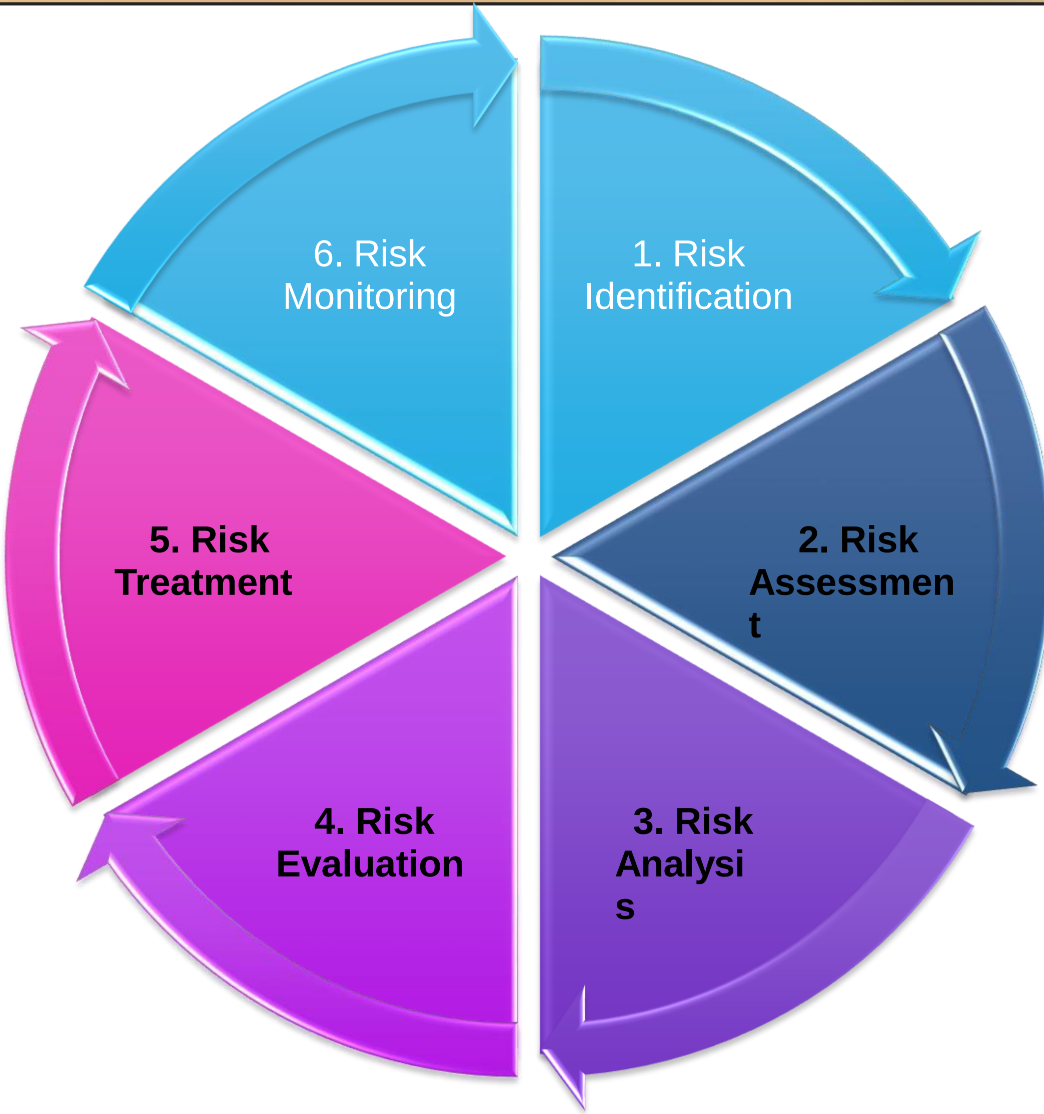
LECTURE 10
RISK ANALYSIS

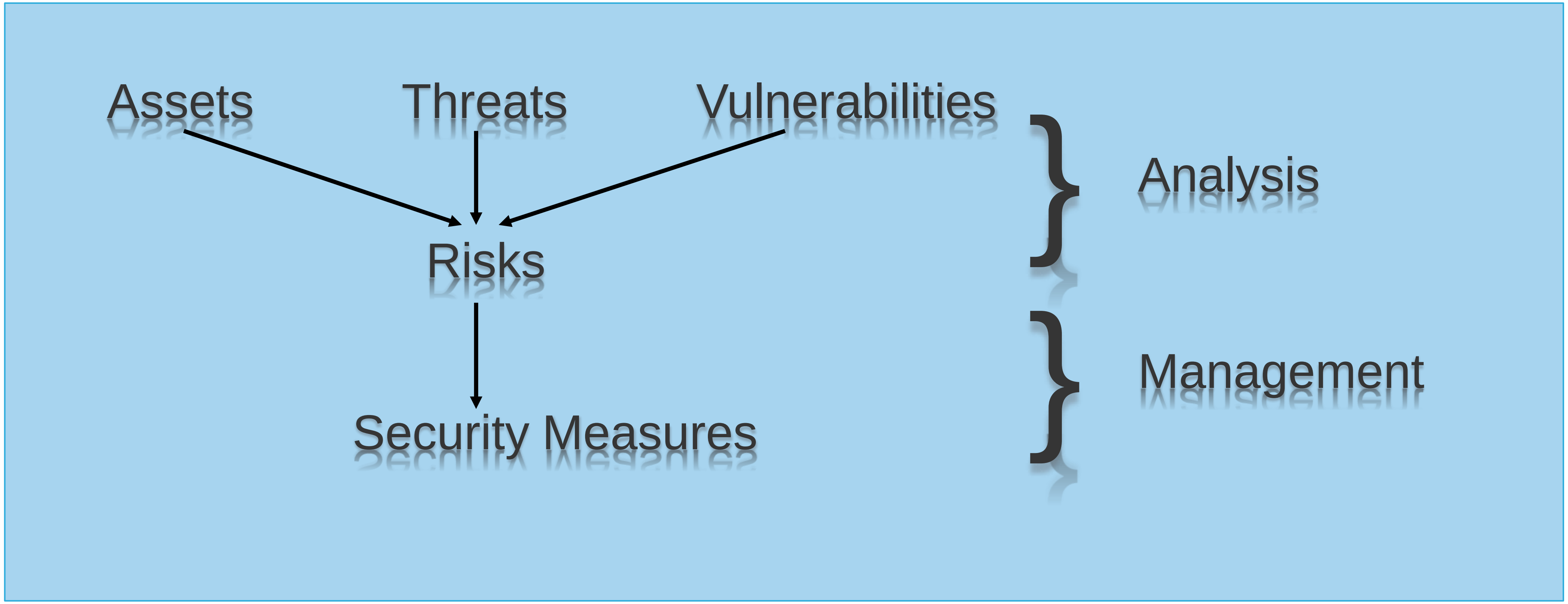
Topics

- Threat analysis
- Vulnerability Analysis
- Likelihood Of Incident
- Consequence Of Incidents

Risk Management



Risk Analysis & Management



Definitions

Risk: a quantified measure of the likelihood of a threat being realised.

- **Risk Analysis** involves the identification and assessment of the levels of risk, calculated from the
  - Values of assets
  - Threats to the assets
  - Their vulnerabilities and likelihood of exploitation

- **Risk Management** involves the identification, selection and adoption of security measures justified by
  - The identified risks to assets
  - The reduction of these risks to acceptable levels

Risk Analysis Types

Quantitative Risk Analysis

- This approach employs two fundamental elements; the probability of an event occurring and the likely loss should it occur.

- Quantitative risk analysis makes use of a single figure produced from these elements. This is called the 'Annual Loss Expectancy (ALE)' or the 'Estimated Annual Cost (EAC)'. This is calculated for an event by simply multiplying the potential loss by the probability.

- Drawbacks:
    - ✓ Usually associated with the unreliability and inaccuracy of the data.
    - ✓ Probability can rarely be precise and can, in some cases, promote complacency.

Risk Analysis Types

Qualitative Risk Analysis

□ This is by far the most widely used approach to risk analysis.

□ Probability data is not required and only estimated potential loss is used.

□ Most qualitative risk analysis methodologies make use of a number of interrelated elements such as THREATS, VULNERABILITIES and CONTROLS

Goal of Risk Analysis

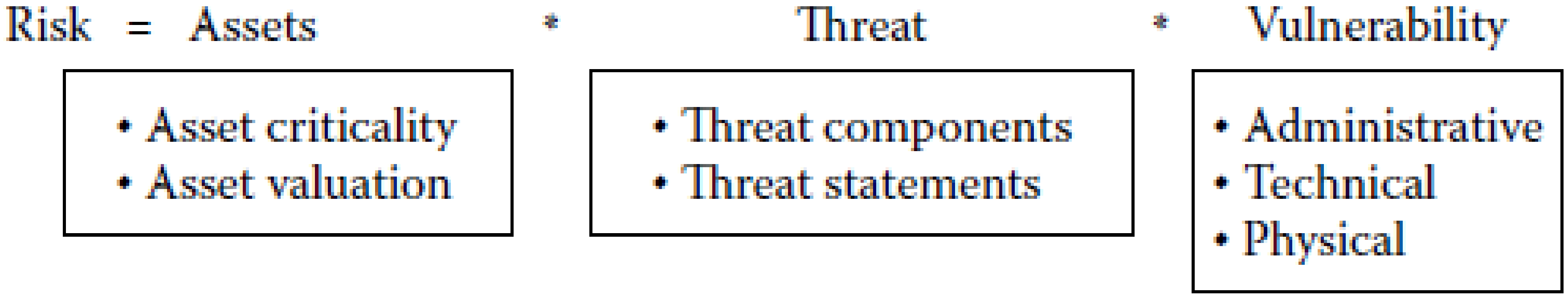
- All assets have been identified
- All threats have been identified
  - Their impact on assets has been valued
- All vulnerabilities have been identified and assessed

Risk Levels

- Precise monetary values give a false precision
- Better to use levels, e.g.
  - High, Medium, Low
    - High: major impact on the organisation
    - Medium: noticeable impact (“material” in auditing terms)
    - Low: can be absorbed without difficulty
  - 1 – 10

- Express money values in levels, e.g.
  - For a large University Department a possibility is
    - High
    - Medium
    - Low

Security Risk Equation



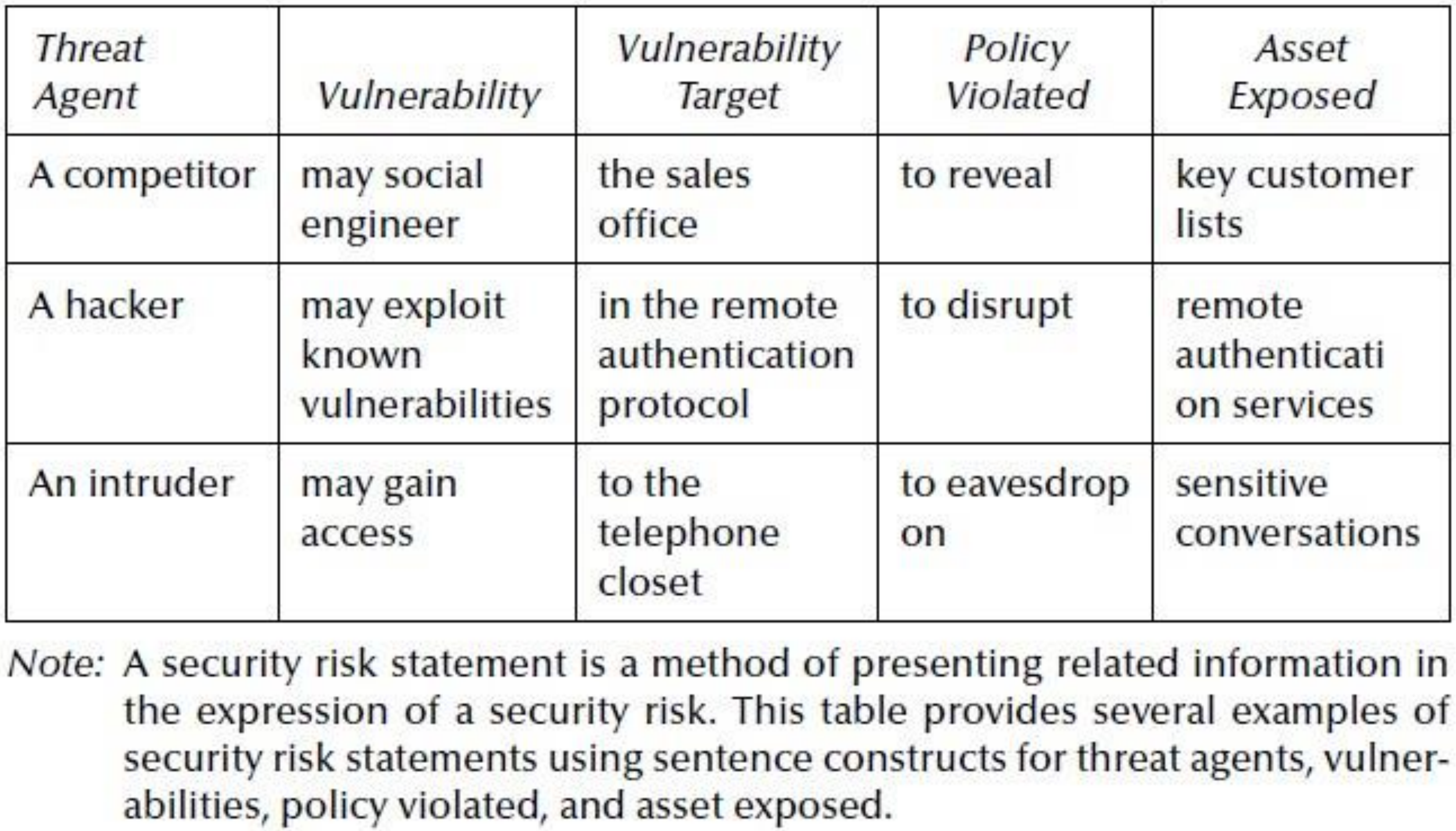
Risk = Assets * Threat * Vulnerability

- Asset criticality
- Asset valuation

- Threat components
- Threat statements

- Administrative
- Technical
- Physical

Creating Security Risk Statement



Threat Agent	*Vulnerability*	*Vulnerability Target*	*Policy Violated*	*Asset Exposed*
A competitor	may social engineer	the sales office	to reveal	key customer lists
A hacker	may exploit known vulnerabilities	in the remote authentication protocol	to disrupt	remote authentication services
An intruder	may gain access	to the telephone closet	to eavesdrop on	sensitive conversations

Note: A security risk statement is a method of presenting related information in the expression of a security risk. This table provides several examples of security risk statements using sentence constructs for threat agents, vulnerabilities, policy violated, and asset exposed.

Risk Analysis Steps

- Decide on scope of analysis
  - Set the system boundary
- Identification of assets & business processes
- Identification of threats and valuation of their impact on assets (*impact valuation*)
- Identification and assessment of vulnerabilities to threats
- Risk assessment

Risk Analysis – Define The Scope

- Draw a context diagram

- Decide on the boundary
  - It will rarely be the computer!

- Make explicit assumptions about the security of neighbouring domains
  - Verify them!

Risk Analysis – Identification of Assets

- Types of asset
  - Hardware
  - Software: purchased or developed programs
  - Data
  - People: who run the system
  - Documentation: manuals, administrative procedures, etc
  - Supplies: paper forms, magnetic media, printer liquid, etc
  - Money
  - Intangibles
    - Goodwill
    - Organization confidence
    - Organisation image

Risk Analysis – Impact Valuation

Identification and valuation of threats - for each group of assets

- Identify threats, e.g. for stored data
  - Loss of **confidentiality**
  - Loss of **integrity**
  - Loss of **completeness**
  - Loss of **availability** (Denial of Service)

- For many asset types the only threat is loss of availability

- Assess impact of threat
  - Assess in levels, e.g H-M-L or 1 - 10
  - This gives the valuation of the asset in the face of the threat

Risk Analysis – Process Analysis

- Every company or organisation has some processes that are critical to its operation
- The criticality of a process may increase the impact valuation of one or more assets identified

So….

- Identify critical processes
- Review assets needed for critical processes
- Revise impact valuation of these assets

Risk Analysis – Vulnerabilities 1

- Identify vulnerabilities against a baseline system
  - For risk analysis of an existing system
    - Existing system with its known security measures andweaknesses
  - For development of a new system
    - Security facilities of the envisaged software, e.g. Windows NT
    - Standard good practice, e.g. BS 7799 recommendations of good practice

Risk Analysis – Vulnerabilities 2

For each threat

- Identify vulnerabilities
  - How to exploit a threat successfully;
- Assess levels of likelihood - High, Medium, Low
  - Of attempt
    - Expensive attacks are less likely (e.g. brute-force attacks on encryption keys)
  - Successful exploitation of vulnerability;
- Combine them

Vulnerability		Likelihood of Attempt		
		Low	Med	High
Likelihood of Success	Low	*Low*	*Low*	*Med*
	Med	*Low*	*Med*	*High*
	High	*Low*	*Med*	*High*

Risk Assessment

Assess risk

- If we had accurate probabilities and values, risk would be
  - Impact valuation x probability of threat x probability of exploitation
  - Plus a correction factor for risk aversion
- Since we haven't, we construct matrices such as

Risk		***Impact valuation***		
		Low	Med	High
Vulnerability	Low	*Low*	*Low*	*Med*
	Med	*Low*	*Med*	*High*
	High	*Low*	*Med*	*High*

Roadmap/Mind Map