# Computer Security course

## Risk Analysis

Erland Jonsson
(based on material from Lawrie Brown)
Department of Computer Science and Engineering
Chalmers University of Technology
Sweden

# Security Management Overview

- **Security requirements** means asking
  - what **assets** do we need to protect?
  - how are those assets **threatened**?
  - what can we do to **counter those threats**?
- **IT Security management** means
  - determine **security objectives** and **risk profile**
  - perform security **risk assessment** of assets
  - select, implement, monitor **controls**

# IT Security Management

- **IT Security Management:** a process used to achieve and maintain **appropriate levels of security** (including confidentiality, integrity, availability, accountability, authenticity and reliability.)
- IT security management functions include:
  - determining organizational IT security **objectives, strategies, policies and security requirements**
  - identifying and **analyzing security threats** to IT assets
  - identifying and **analyzing risks**
  - specifying appropriate **safeguards**
  - **implementation and operation of safeguards**
  - developing and implement a **security awareness program**
  - **incident handling**

# ISO 27000 Security Standards

| | |
|---|---|
| **ISO27000** | a proposed standard which will define the vocabulary and definitions used in the 27000 family of standards. |
| **ISO27001** | defines the information security management system specification and requirements against which organizations are formally certified. It replaces the older Australian and British national standards AS7799.2 and BS7799.2. |
| **ISO27002 (ISO17799)** | currently published and better known as ISO17799, this standard specifies a code of practice detailing a comprehensive set of information security control objectives and a menu of best-practice security controls. It replaces the older Australian and British national standards AS7799.1 and BS7799.1. |
| **ISO27003** | a proposed standard containing implementation guidance on the use of the 27000 series of standards following the "Plan-Do-Check-Act" process quality cycle. Publication is proposed for late 2008. |
| **ISO27004** | a draft standard on information security management measurement to help organizations measure and report the effectiveness of their information security management systems. It will address both the security management processes and controls. Publication is proposed for 2007. |
| **ISO27005** | a proposed standard on information security risk management. It will replace the recently released British national standard BS7799.3. Publication is proposed for 2008/9. |
| **ISO13335** | provides guidance on the management of IT security. This standard comprises a number of parts. Part 1 defines concepts and models for information and communications technology security management. Part 2, currently in draft, will provide operational guidance on ICT security. These replace the older series of 5 technical reports ISO/IEC TR 13335 parts 1-5. |

# Risk assessment approaches

- Baseline approach
  - Implements a basic general level of security controls and industry best practice ("best effort")
  - identify likelihood of risk and consequences
  - hence have confidence controls appropriate
- Informal approach
  - Some kind of informal, pragmatic risk analysis (mainly for SMEs), cheap and fast
- Detailed risk analysis
  - uses a formal structured process
- Combined approach

# Detailed Risk Analysis

- most comprehensive alternative
- assess using formal structured process
  - with a number of stages
  - identify likelihood of risk and consequences
  - hence have confidence controls appropriate
- costly and slow, requires expert analysts
- may be a legal requirement to use
- suitable for large organizations with IT systems critical to their business objectives

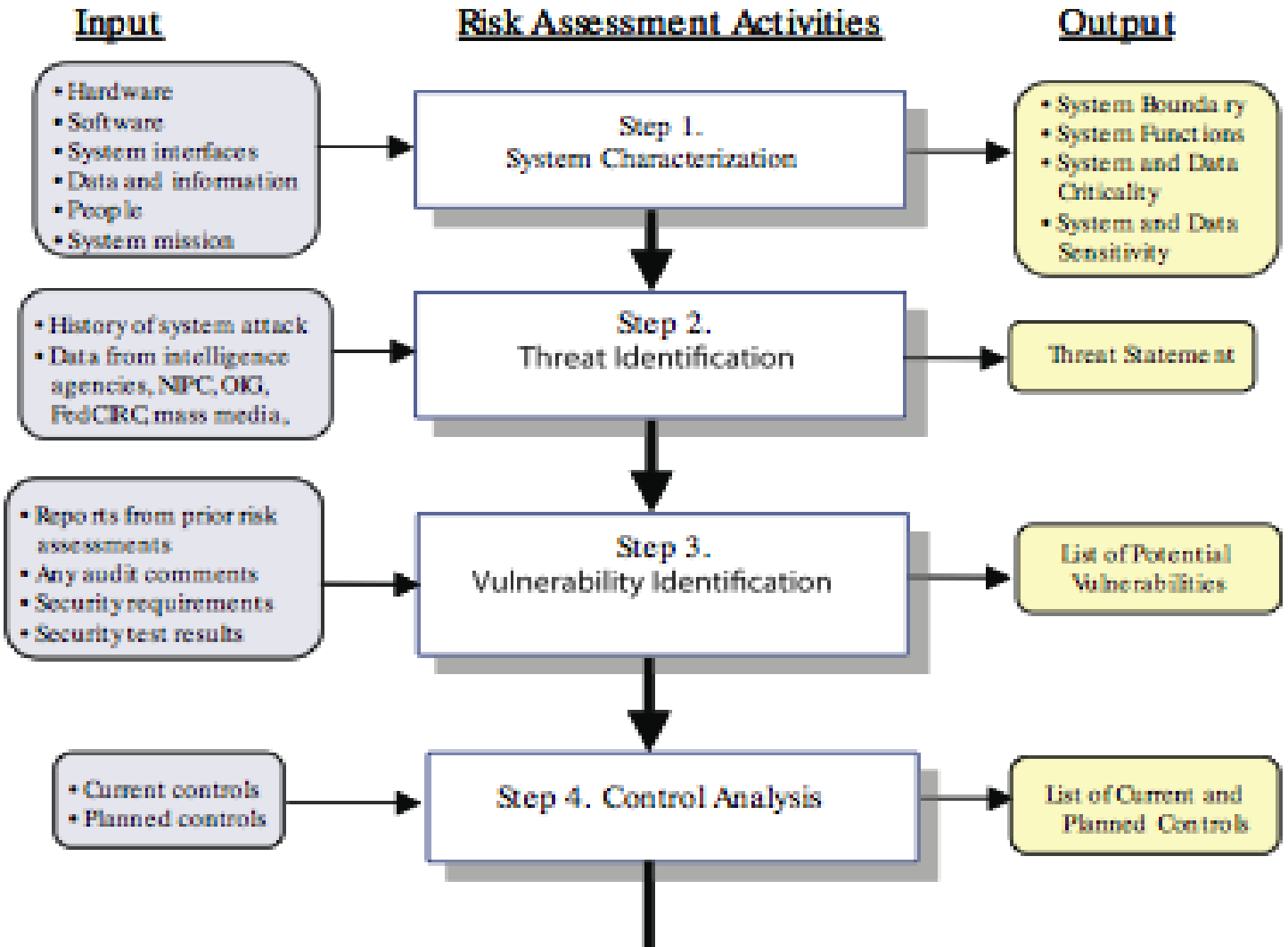
# Detailed Risk Analysis Process
## - outline

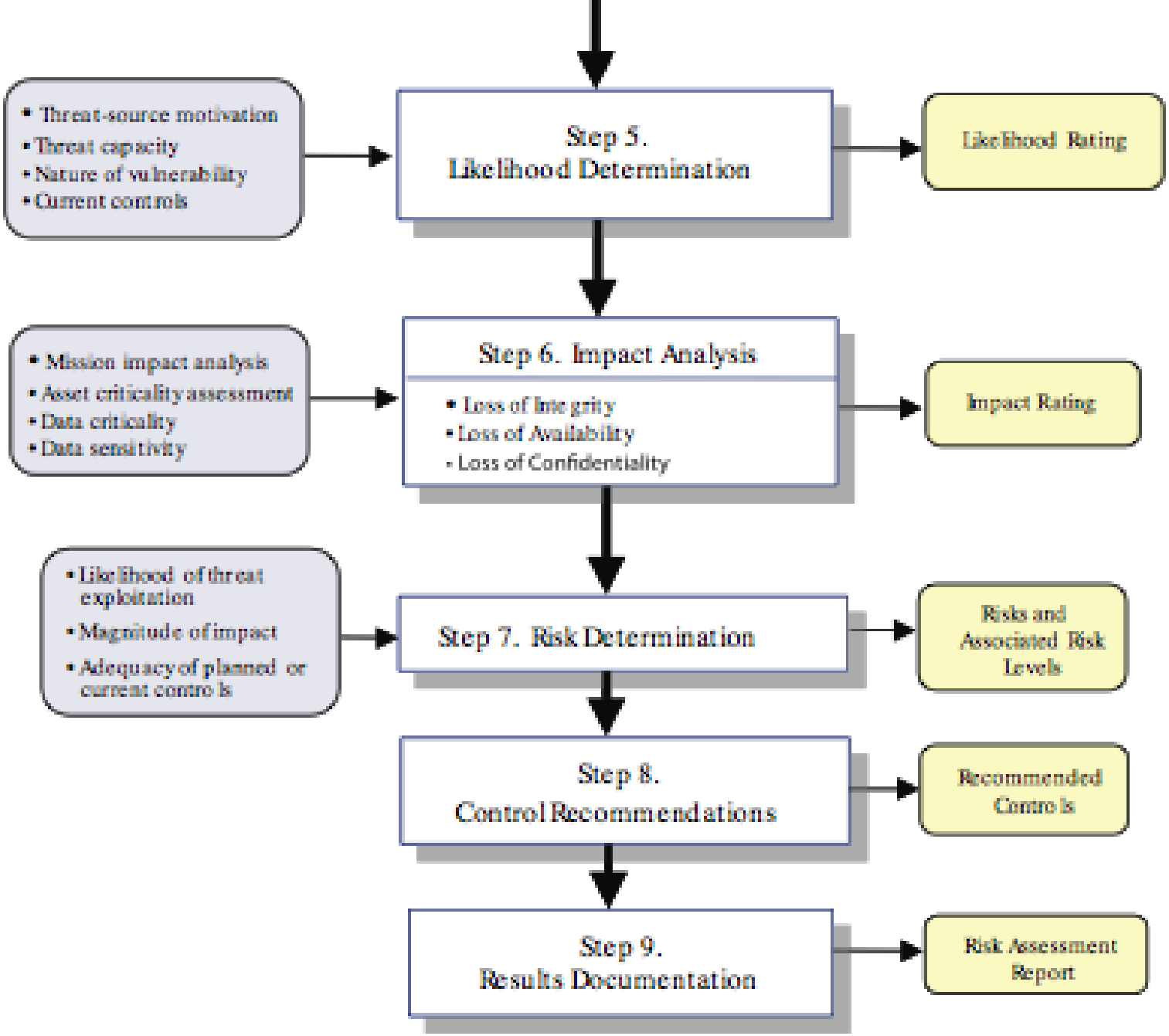
- Prepare/check status

- Identify threat sources
- Identify vulnerabilities
- Determine likelihood
- Determine impact (consequences)
- Determine risk

- Take action

# Risk Assessment Process




• Threat-source motivation
• Threat capacity
• Nature of vulnerability
• Current controls
Step 5.
Likelihood Determination
Likelihood Rating
• Mission impact analysis
• Asset criticality assessment
• Data criticality
• Data sensitivity
Step 6. Impact Analysis
• Loss of Integrity
• Loss of Availability
• Loss of Confidentiality
Impact Rating
• Likelihood of threat exploitation
• Magnitude of impact
• Adequacy of planned or current controls
Step 7. Risk Determination
Risks and Associated Risk Levels
Step 8.
Control Recommendations
Recommended Controls
Step 9.
Results Documentation
Risk Assessment Report

# Establish Context

- determine the broad risk exposure of the organisation
  - related to wider political / social environment
  - and legal and regulatory constraints
  - provide baseline for organization's risk exposure
- specify organization's risk appetite
- set boundaries of risk assessment
  - partly based on risk assessment approach used
- decide on risk assessment criteria used

# Asset Identification

- identify assets
  - "anything which needs to be protected"
  - items of value to organization to meet its objectives
  - tangible or intangible
  - in practice try to identify significant assets
- draw on expertise of people in relevant areas of organization to identify key assets
  - identify and interview such personnel
  - see checklists in various standards

# Threat Identification

- threats are anything that hinders or prevents an asset to provide the appropriate levels of the key security services:
  - confidentiality, integrity, availability, accountability, authenticity and reliability
- to identify threats or risks to assets, ask
  1. who or what could cause it harm?
  2. how could this occur?
- assets may have multiple threats

# Threat Identification

- Consider reasons and capabilities for human threat sources
  - motivation (why?, goals, rewards)
  - capability (skill)
  - resources (time, tools, money, etc)
  - deterrence (e.g. possible lawsuit)
  - probability of an attack
    (ab. the combination of the above)

# Vulnerability Identification

- identify exploitable flaws or weaknesses in organization's IT systems or processes
- hence determine applicability and significance of threat to organization
- note that you need a combination of a threat and a vulnerability to create a risk to an asset
- use lists of potential vulnerabilities in standards etc

# Analyse Risks

- specify **likelihood of occurrence** of each identified threat to asset given existing controls
  - management, operational, technical processes and procedures to reduce risk exposure
- specify **consequence** should the threat occur
- hence **derive overall risk rating** for each threat:
  **risk =**
  **probability threat occurs x cost to organization**
- in practice very hard to determine probabilities exactly, thus you may need to use qualitative (rather than quantitative) ratings for each
- aim to order resulting risks in order to treat them

# Determine Likelihood

| Rating | Likelihood Description | Expanded Definition |
|---|---|---|
| 1 | **Rare** | May occur only in exceptional circumstances and may deemed as “unlucky” or very unlikely. |
| 2 | **Unlikely** | Could occur at some time but not expected given current controls, circumstances, and recent events. |
| 3 | **Possible** | Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences. |
| 4 | **Likely** | Will probably occur in some circumstance and one should not be surprised if it occurred. |
| 5 | **Almost Certain** | Is expected to occur in most circumstances and certainly sooner or later. |

# Determine Consequence

| Rating | Consequence | Expanded Definition. |
|---|---|---|
| 1 | **Insignificant** | Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify. |
| 2 | **Minor** | Result of a security breach in one or two areas. Impact is likely to last less than a week, but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources. |
| 3 | **Moderate** | Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and generally requires management intervention. Will have ongoing compliance costs to overcome. |
| 4 | **Major** | Ongoing systemic security breach. Impact will likely last 4-8 weeks and require significant management intervention and resources to overcome, and compliance costs are expected to be substantial. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off. |
| 5 | **Catastrophic** | Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action is likely. |
| 6 | **Doomsday** | Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable. |

# Determine Resultant Risk Level

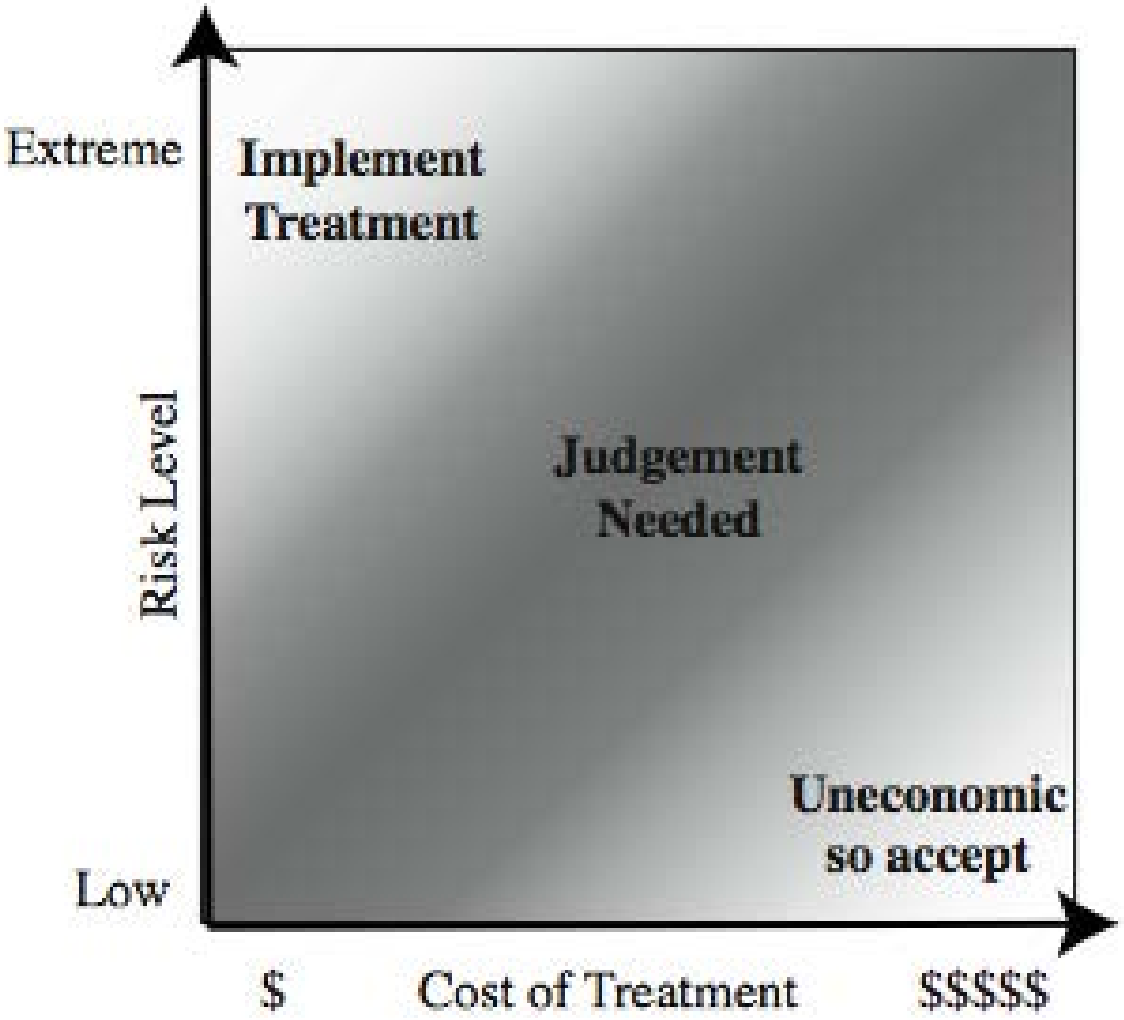
| | Consequences | | | | | |
|---|---|---|---|---|---|---|
| **Likelihood** | **Doomsday** | **Catastrophic** | **Major** | **Moderate** | **Minor** | **Insignificant** |
| **Almost Certain** | E | E | E | E | H | H |
| **Likely** | E | E | E | H | H | M |
| **Possible** | E | E | E | H | M | L |
| **Unlikely** | E | E | H | M | L | L |
| **Rare** | E | H | H | M | L | L |

| Risk Level | Description |
|---|---|
| **Extreme (E)** | Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts. |
| **High (H)** | Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources. |
| **Medium (M)** | Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews. |
| **Low (L)** | Can be managed through routine procedures. |

# Document in Risk Register and Evaluate Risks

| Asset | Threat/ Vulnerability | Existing Controls | Likelihood | Consequence | Level of Risk | Risk Priority |
|---|---|---|---|---|---|---|
| Internet Router | Outside Hacker attack | Admin password only | Possible | Moderate | High | 1 |
| Destruction of Data Center | Accidental Fire or Flood | None (no disaster recovery plan) | Unlikely | Major | High | 2 |

# Risk Treatment Alternatives



# Risk Treatment Alternatives

Three major alternatives for risk treatment:

- risk acceptance – "take the risk"
- risk avoidance – "do not do it"
- risk transferral – "insure yourself, look for partners"

Plus two alternatives that are really "normal" security measures:

- reduce consequence – "back-ups, recovery plans"
- reduce likelihood – "better security mechanisms and controls"

# Summary

- **risk assessment** is an important part of the IT security management process
- detailed risk assessment process involves
  - context including asset identification
  - identify threats, vulnerabilities, risks
  - analyse and evaluate risks
- deal with the risk assessment correctly