Universitas Esa Unggul

Smart, Creative and Entrepreneurial

Analisis Resiko Sistem Informasi

Risk Analysis Methodology 1

www.esaunggul.ac.id

Pertemuan 3

Dosen Pengampu: Alivia Yulfitri (2017)

Prodi Sistem Informasi - Fakultas Ilmu Komputer

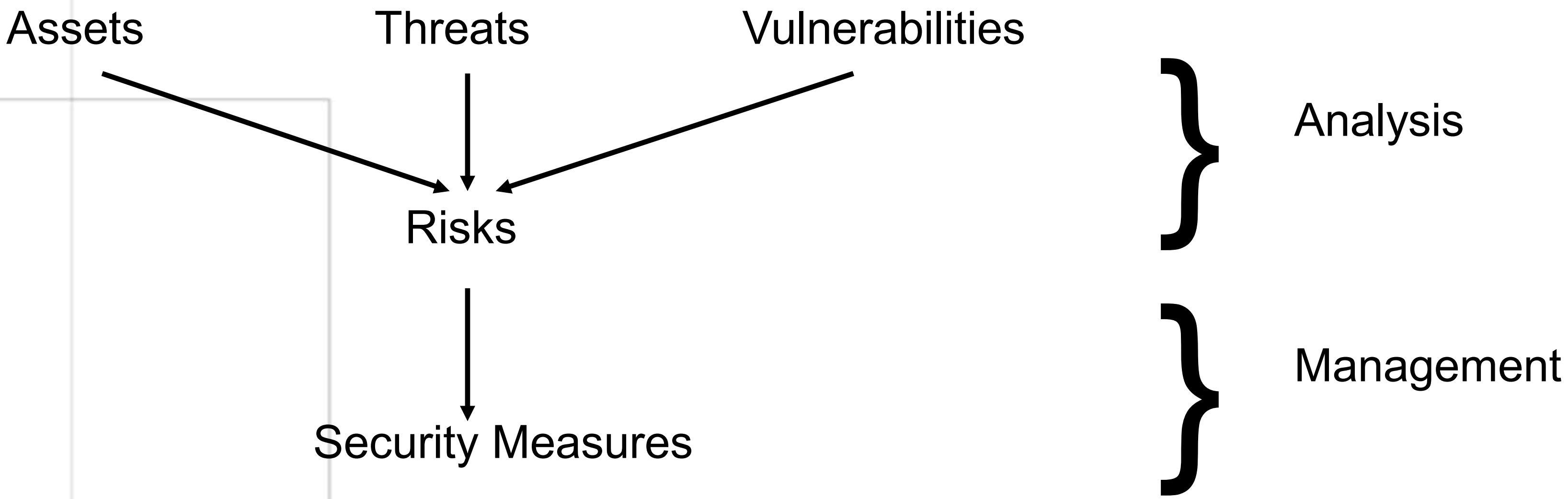
Risk Assessment: Methodology

When to perform?

- **Periodically**
  - Often event-driven
  - Typically year-over-year comparison
  - Generally labor-intensive
  - Most organizations start with periodic assessments
- **Continuously**
  - Part of the normal workflow
  - Provides “real-time” risk view
  - Often supported by technology and analysis tools
  - Integrated with other IT/business processes

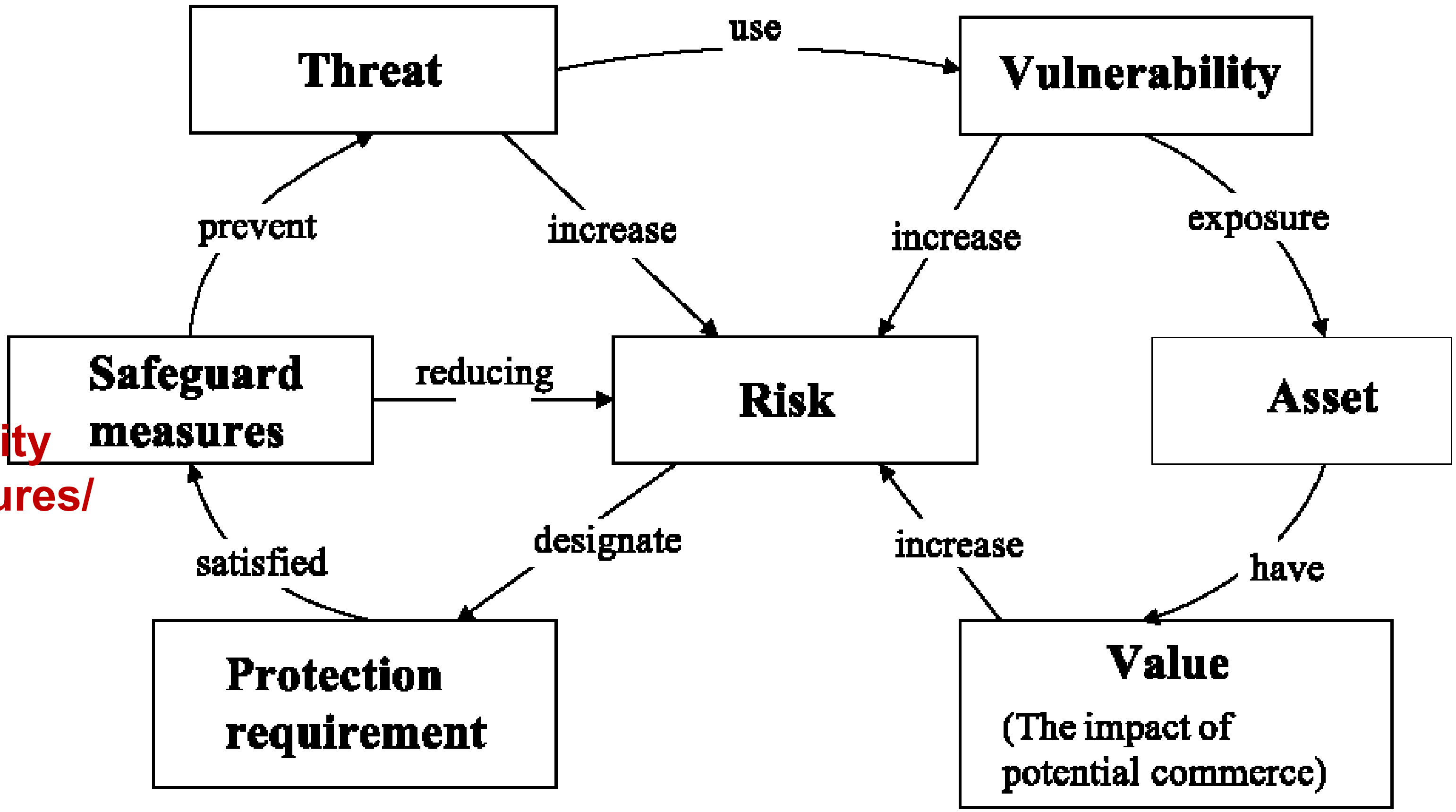
Introduction

Risk Analysis and Management Framework



Risk Analysis

Conceptualisation map of Information System



Threat

use

Vulnerability

prevent

increase

increase

exposure

Safeguard measures

reducing

Risk

Asset

satisfied

designate

increase

have

Protection requirement

Value

(The impact of potential commerce)

Security Measures/

Source: Australian Standard Handbook of Information Security Risk Management – HB231-2000

Definitions

The meanings of terms in this area is not universally agreed. We will use the following

- **Threat**: Harm that can happen to an asset
- **Impact**: A measure of the seriousness of a threat
- **Attack**: A threatening event
- **Attacker**: The agent causing an attack (not necessarily human)
- **Vulnerability**: a weakness in the system that makes an attack more likely to succeed
- **Risk**: a quantified measure of the likelihood of a threat being realised

Goals of Risk Analysis

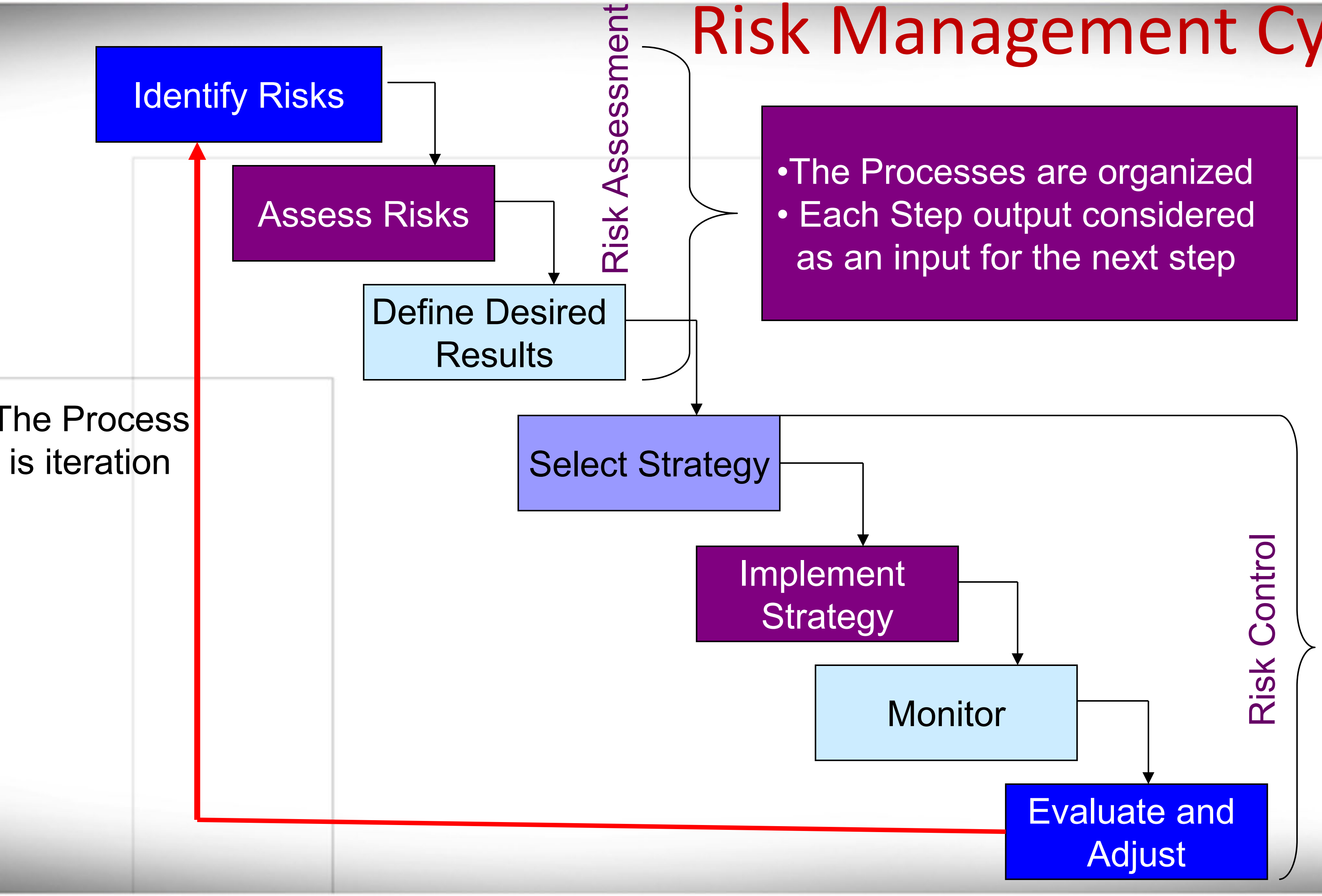
- All assets have been identified
- All threats have been identified
    - Their impact on assets has been valued
- All vulnerabilities have been identified and assessed

Problems of Measuring Risk

Businesses normally wish to measure in money, but

- Many of the entities do not allow this
  - Valuation of assets
    - Value of data and in-house software - no market value
    - Value of goodwill and customer confidence
  - Likelihood of threats
    - How relevant is past data to the calculation of future probabilities?
      - The nature of future attacks is unpredictable
      - The actions of future attackers are unpredictable
  - Measurement of benefit from security measures
    - Problems with the difference of two approximate quantities
      - How does an extra security measure affect a ~10^{-5} probability of attack?

Risk Management Cycle



- The Processes are organized
- Each Step output considered as an input for the next step

Methods of Risk Analysis

There are various methods analysing risk:

First : Quantitative risk analysis:

generally estimates values of Information Systems components as ; information, systems, business processes, recovery costs, etc.,

risk can be measured in terms of direct and indirect costs , based on

(1) the likelihood that a damaging event will occur

(2) the costs of potential losses

(3) the costs of mitigating actions that could be taken.

Second : Qualitative Risk Assessment

This approach can be taken by defining

- **Risk in more subjective and general terms such as high, medium, and low.**
- **In this regard, qualitative analysis depend more on the *expertise, experience, and judgment of those conducting the assessment*.**

- Qualitative risk analysis typically give risk results of “High”, “Moderate” and “Low”. However, by providing the impact and likelihood definition tables and the description of the impact, it is possible to adequately communicate the assessment to the organization’s management.

Third :Quantitative and Qualitative

– It is also possible to use a combination of quantitative and qualitative method

Risk Analysis: Methodology

Key Steps

1. Define objectives

2. Define deliverables

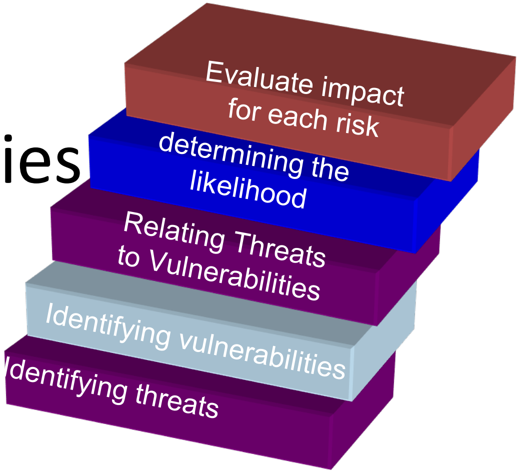
3. Establish a work plan -> Methodology

4. Determine tools to assist with process

How to assess the risks

Risk is assessed by following the following steps:

1. Identifiying assets
2. Identifying threats and impact
3. Identifying vulnerabilities
4. Relating Threats to Vulnerabilities
5. determining the likelihood
6. Evaluate impact for each risk


Evaluate impact for each risk
determining the likelihood
Relating Threats to Vulnerabilities
Identifying vulnerabilities
Identifying threats

1. 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
    - Organisation confidence
    - Organisation image

1. Risk Analysis - Identification of Assets

Outline

- What are tangible assets?
- What are non-tangible assets?
- How to assign value to assets?
- What questions should be asked?
- Example
  - Lemonade Stand

Identification of Assets

Tangible

- **Assets**- Something that the agency values and has to protect. Assets include all information and supporting items that an agency requires to conduct business.

1. Hardware
   – Processors, boards, monitors, keyboards, terminals, drives, cables, connections, controllers, communications media, etc.
2. Software: purchased or developed programs
   – Source programs, object programs, purchased programs, operating systems, systems programs, diagnostic programs, etc.
3. Information/Data
   – Data used during execution, stored data on various media, archival records, audit data, files with payment details, voice records, image files, product information, continuity plans.
4. Services
   – Provided by the company. (e.g. computing and communication services, service providers and utilities)
5. Documentation
   – On programs, hardware, systems, administrative procedures and the entire system, contracts, completed forms.

Identification of Assets

Non-Tangible

1. People and their knowledge (Employees)
   – Integral function/skills which the employee provides (e.g. technical, operational, marketing, legal, financial, contractors/consultants, outsourced providers)

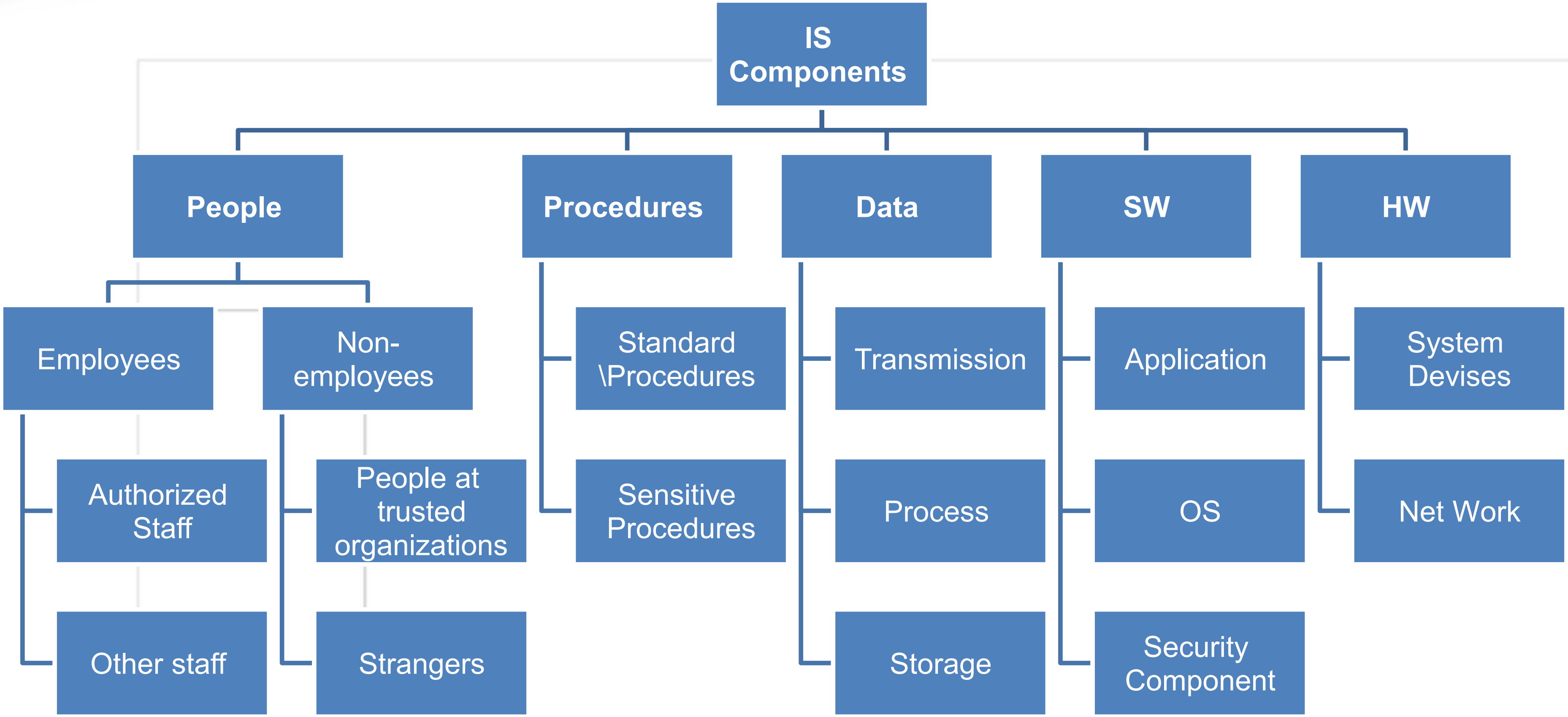
2. Reputation and Image
   – Value attributed to an organization as a result of its general estimation in the public eye. (e.g. political standing in the case of government agencies)

3. Trust
   – Value consistent with public opinion on the integrity and character of an organization.

1. Intellectual Property
   – Any product of the human intellect that is unique, novel, and unobvious (and has some value in the marketplace)

Source: http://www.uta.edu/tto/ip-defs.htm

Information Assets



- IS Components
  - People
    - Employees
      - Authorized Staff
      - Other staff
    - Non-employees
      - People at trusted organizations
      - Strangers
  - Procedures
    - Standard \Procedures
    - Sensitive Procedures
  - Data
    - Transmission
    - Process
    - Storage
  - SW
    - Application
    - OS
    - Security Component
  - HW
    - System Devises
    - Net Work

Determine Assets

Valuation

- Asset values are used to identify the appropriate protection of assets and to determine the importance of the assets to the business.
- Values can be expressed in terms of:
  - Potential business impacts affecting loss of confidentiality, integrity and availability.
- Valuation of some assets different for small and large organizations
- Intangible assets hard to quantify
- Hidden costs of damages to recovery (often underestimated)

Determine Assets

Valuation, cont'd.

- In this step, ramifications of failure on organization are determined.
- Often inaccurate
  - Costs of human capital required to recover from failure undervalued e.g. cost of restoring data
  - Indirect consequences of an event unknown until the event actually happens
  - Catastrophic events that cause heavy damage are so infrequent that correct data unavailable
  - Non-tangible assets hard to quantify
- The questions on the next slide prompt us to think about issues of explicit and hidden cost related to security.
  - The answers may not produce precise cost figures, but help identify sources of various types of costs.

Determine Assets

Guiding Questions to Reflect on Intangible Assets

- What are the legal obligations in preserving confidentiality or integrity of data?
- What business requirements and agreements cover the situation?
- Could release of a data item cause harm to a person or organization?
- Could unauthorized access to data cause loss of future business opportunity?
- What is the psychological effect of lack of computer service?
- What is the value of access to data or programs?
- What is the value of having access to data or programs to someone else?
- What other problems would arise from loss of data?

Determine Assets

General Example #1: Lemonade Stand

Billy sells lemonade outside of his house every weekend for 3 hours a day. Every week he makes about $40. The wooden stand has a cardboard sign which reads, "Lemonade for SALE, 25 cents each". Supplies he receives from his mother are paper cups and a glass pitcher and spoon to stir with. For one pitcher of lemonade, he needs 4 lemons, 2 cups of sugar, 1 quart of water, and a secret ingredient and 10 minutes. The special recipe is located in a small space within the lemonade stand. He has a general crowd of about 10 neighbors who buy from him because they enjoy the taste of his lemonade and his personality.

Determine Assets

General Example #1: Lemonade Stand, cont’d.

Listing of Tangible Assets:

- Establishment
  - Lemonade stand: $5
- Advertising
  - Sign: $1
- Supplies
  - Pitcher: $7
  - Paper cups: $2/25 pack
  - Spoon: $1.50
  - Lemons: $3/10 pack
  - Sugar: $1/1 lb.
  - Water: $1/gallon
  - Secret ingredient: $1/1 lb.

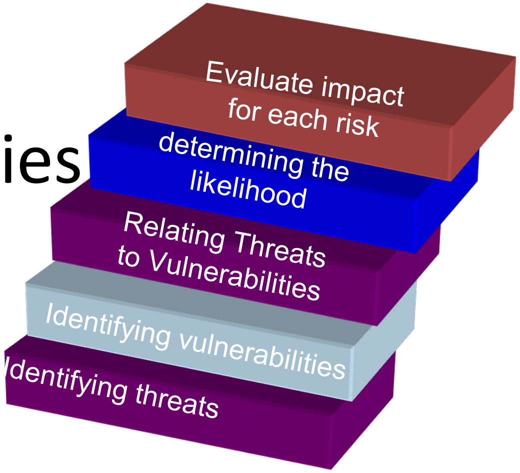
Listing of Intangible Assets:

- People
  - Billy
  - Billy’s Mother
- Intellectual Property
  - Special recipe
- Trust
- Reputation
- Customer base

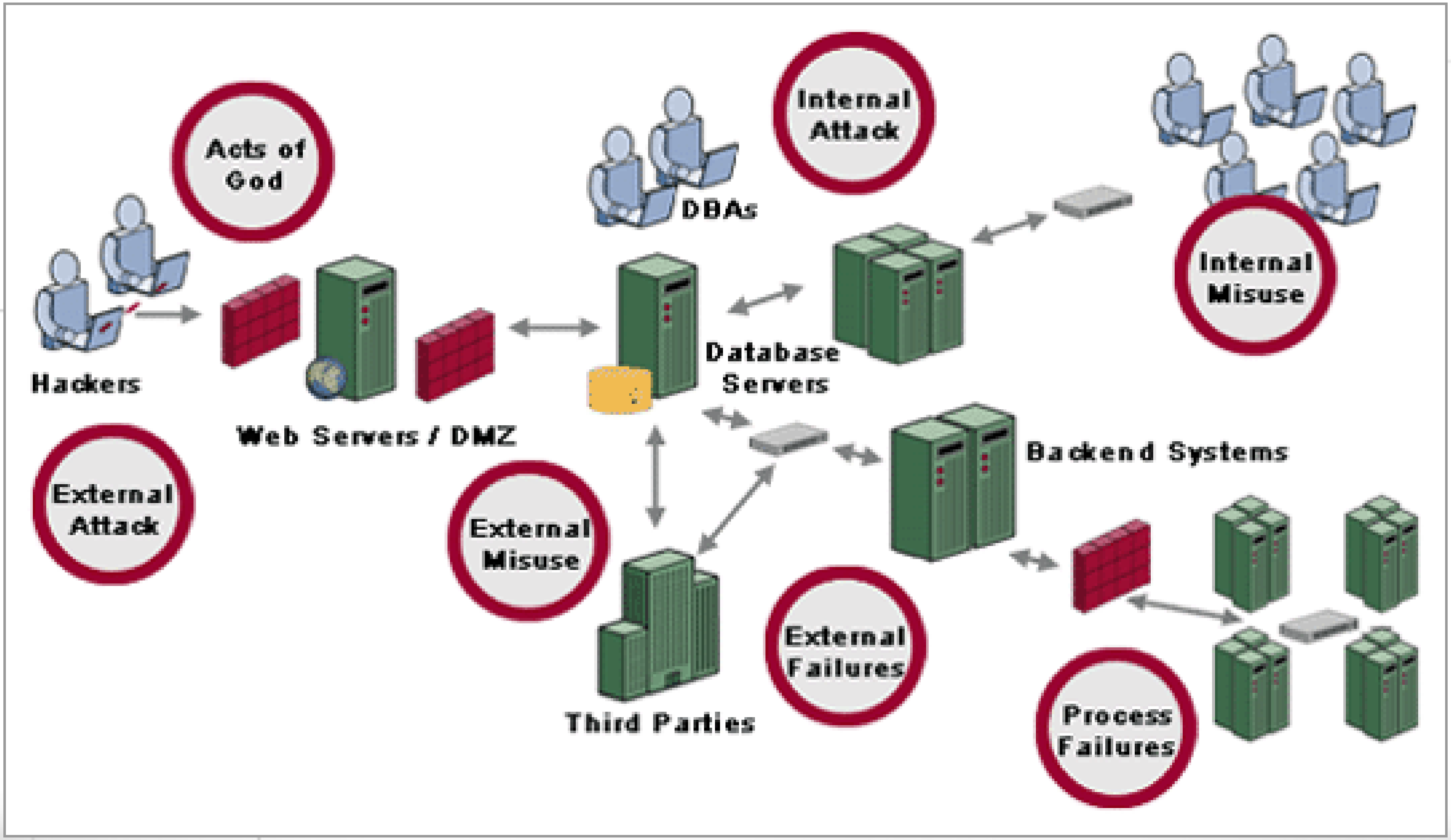
How to assess the risks

Risk is assessed by following the following steps:

1. Identifiying assets
2. Identifying threats and impact
3. Identifying vulnerabilities
4. Relating Threats to Vulnerabilities
5. determining the likelihood
6. Evaluate impact for each risk


Evaluate impact for each risk
determining the likelihood
Relating Threats to Vulnerabilities
Identifying vulnerabilities
Identifying threats

2. Identifying Threats and Impact



Identification of Threats

- **Threat-** Potential cause of an unwanted event that may result in harm to the agency and its assets. A threat is a manifestation of vulnerability.
- Malicious
  - Malicious Software (Viruses, worms, trojan horses, time bomb logic bomb, rabbit, bacterium)
  - Spoofing or Masquerading
  - Sequential or Dictionary Scanning
  - Snooping (electronic monitoring or “shoulder surfing”)
  - Scavenging (“dumpster diving” or automated scanning of data)
  - Spamming
  - Tunneling
- Unintentional
  - Equipment or Software Malfunction
  - Human error (back door or user error)
- Physical
  - Power loss, vandalism, fire/flood/lightning damage, destruction

Identifying Threat and Impact (cont)

Identification and valuation of threats - for each group of assets

- Identify threats, e.g. for stored data
  - Loss of **confidentiality:** Someone sees your password or a company's "secret formula"
  - Loss of **integrity:** An email message is modifed in transit, a virus infects a fle, or someone makes unauthorized changes to a Web site.
  - Loss of **availability** (Denial of Service): An email server is down and no one has email access, or a fle server is down so data fles aren't available
- 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

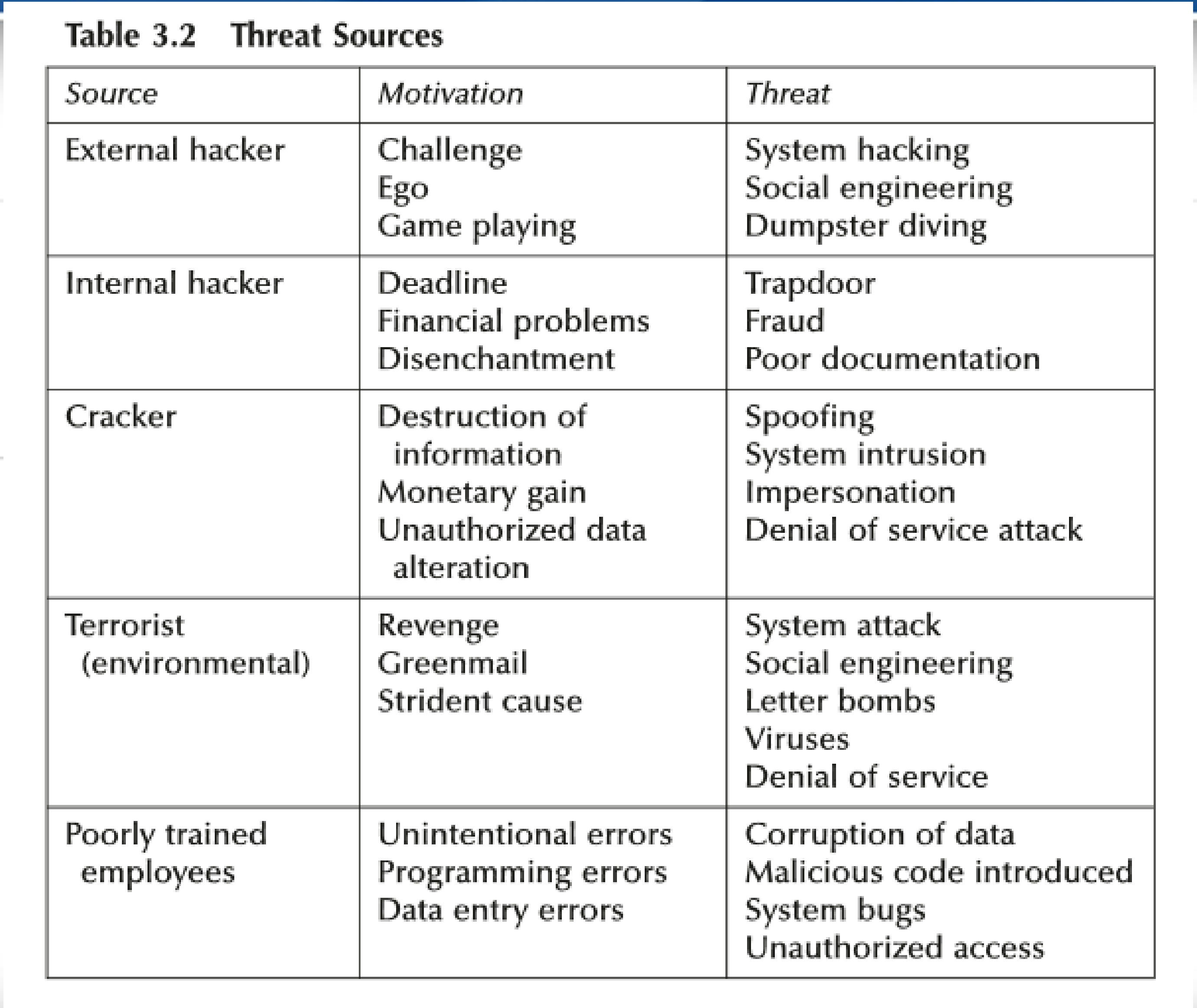


Table 3.2 Threat Sources

Source	*Motivation*	*Threat*
External hacker	Challenge Ego Game playing	System hacking Social engineering Dumpster diving
Internal hacker	Deadline Financial problems Disenchantment	Trapdoor Fraud Poor documentation
Cracker	Destruction of information Monetary gain Unauthorized data alteration	Spoofing System intrusion Impersonation Denial of service attack
Terrorist (environmental)	Revenge Greenmail Strident cause	System attack Social engineering Letter bombs Viruses Denial of service
Poorly trained employees	Unintentional errors Programming errors Data entry errors	Corruption of data Malicious code introduced System bugs Unauthorized access

- Source: Information Security Risk Analysis, Peltier

THREAT IMPACTS

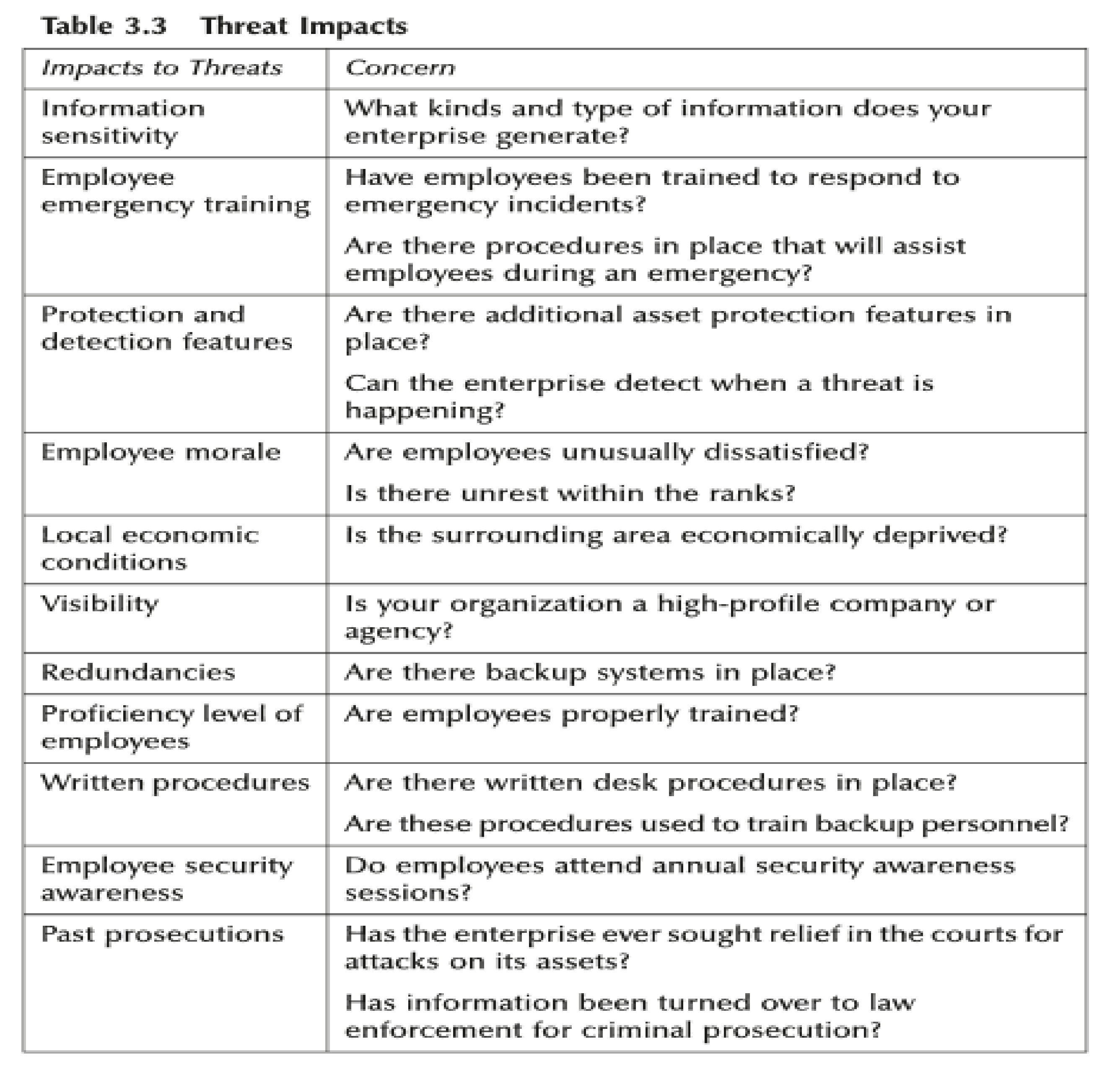


Table 3.3 Threat Impacts

Impacts to Threats	*Concern*
Information sensitivity	What kinds and type of information does your enterprise generate?
Employee emergency training	Have employees been trained to respond to emergency incidents? Are there procedures in place that will assist employees during an emergency?
Protection and detection features	Are there additional asset protection features in place? Can the enterprise detect when a threat is happening?
Employee morale	Are employees unusually dissatisfied? Is there unrest within the ranks?
Local economic conditions	Is the surrounding area economically deprived?
Visibility	Is your organization a high-profile company or agency?
Redundancies	Are there backup systems in place?
Proficiency level of employees	Are employees properly trained?
Written procedures	Are there written desk procedures in place? Are these procedures used to train backup personnel?
Employee security awareness	Do employees attend annual security awareness sessions?
Past prosecutions	Has the enterprise ever sought relief in the courts for attacks on its assets? Has information been turned over to law enforcement for criminal prosecution?

- Source: Information Security Risk Analysis, Peltier

- One of the most basic forms of risk analysis is a process known as an annual loss exposure (ALE).
- The ALE takes the value (V) of an asset and then uses the likelihood (L) of a threat occurrence in a formula to calculate the ALE:

$$V \times L = ALE$$

- The ALE would work like this: You have a $3 million data center located in a flood area. A major flood that would destroy the data center occurs once every 100 years. Value = $3 million Likelihood = Once every 100 years (using the table above, L = 0.01) $3 million × 0.01 = $30,000

- Insurance companies use the ALE to assist them in determining what kind of premium they should charge. For the risk management professional, this form of risk analysis is often misleading. The loss if a flood occurs is not $30,000, but actually $3,000,000.

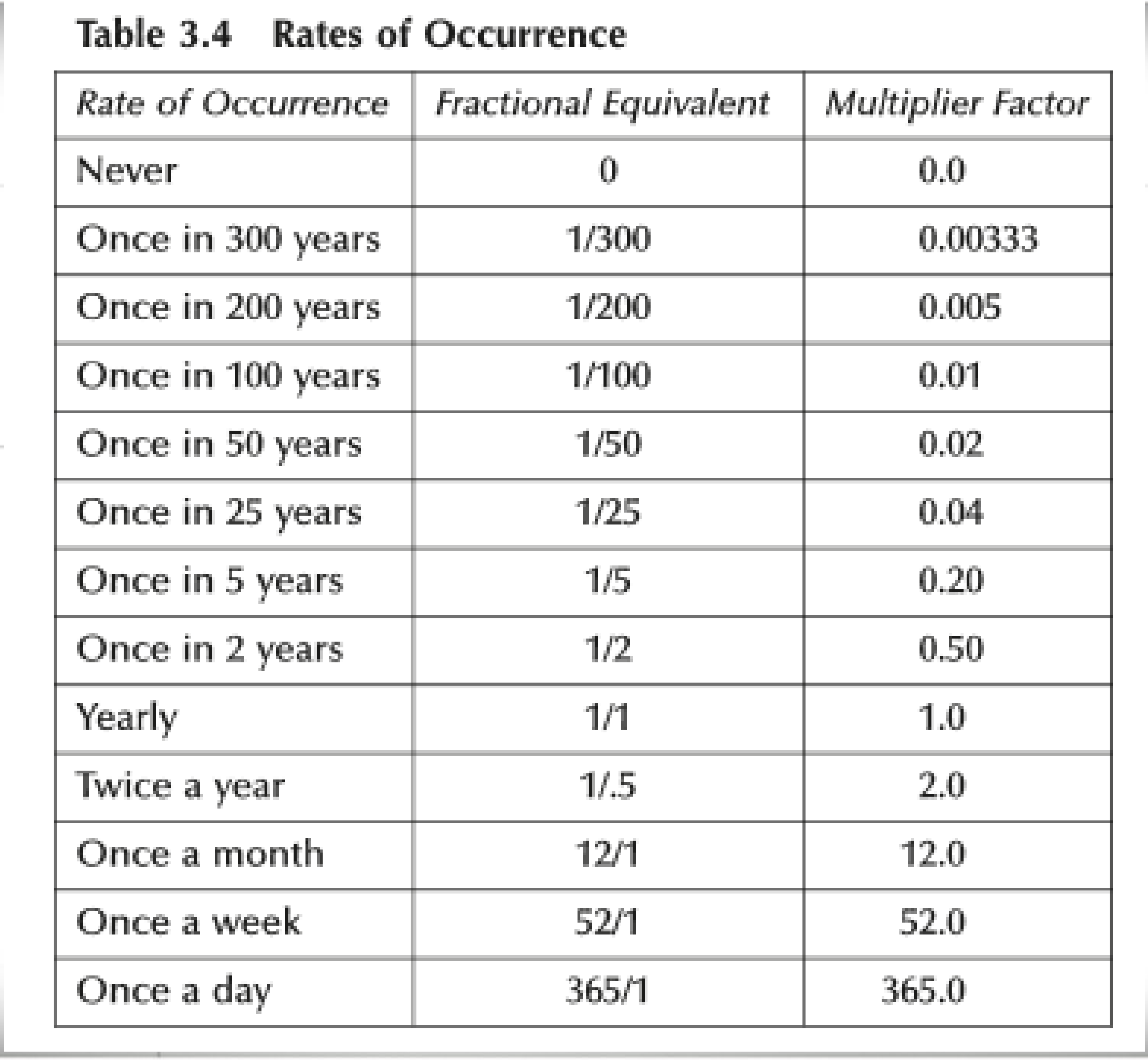


Table 3.4 Rates of Occurrence

Rate of Occurrence	*Fractional Equivalent*	*Multiplier Factor*
Never	0	0.0
Once in 300 years	1/300	0.00333
Once in 200 years	1/200	0.005
Once in 100 years	1/100	0.01
Once in 50 years	1/50	0.02
Once in 25 years	1/25	0.04
Once in 5 years	1/5	0.20
Once in 2 years	1/2	0.50
Yearly	1/1	1.0
Twice a year	1/.5	2.0
Once a month	12/1	12.0
Once a week	52/1	52.0
Once a day	365/1	365.0

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

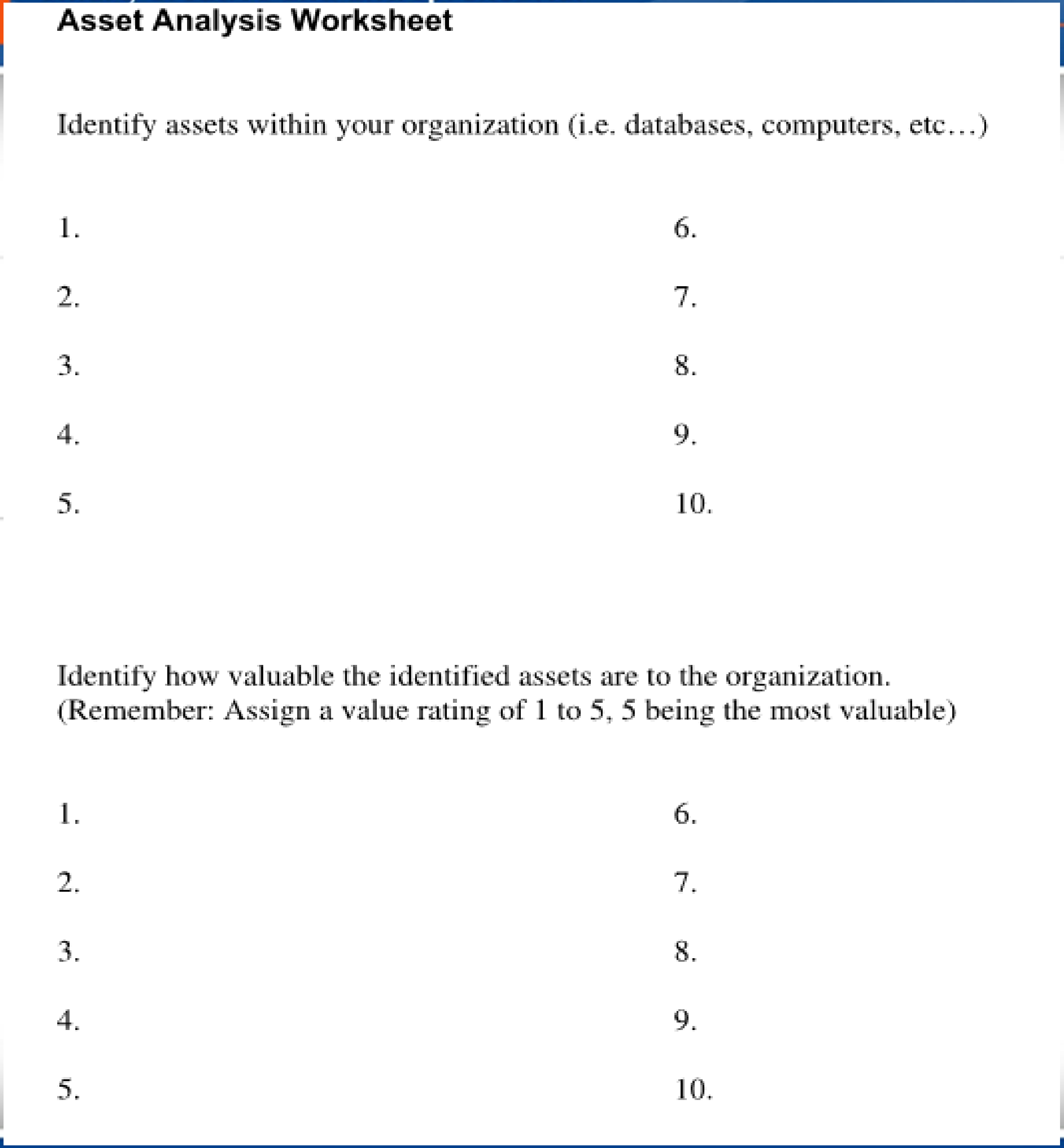
So

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

Identifying Assets and Threats

Assignment

- Using your own organization, determine the assets and threats and impact.
- Fill the worksheet for assets (see next slide)
- Fill the worksheet for threat and impact



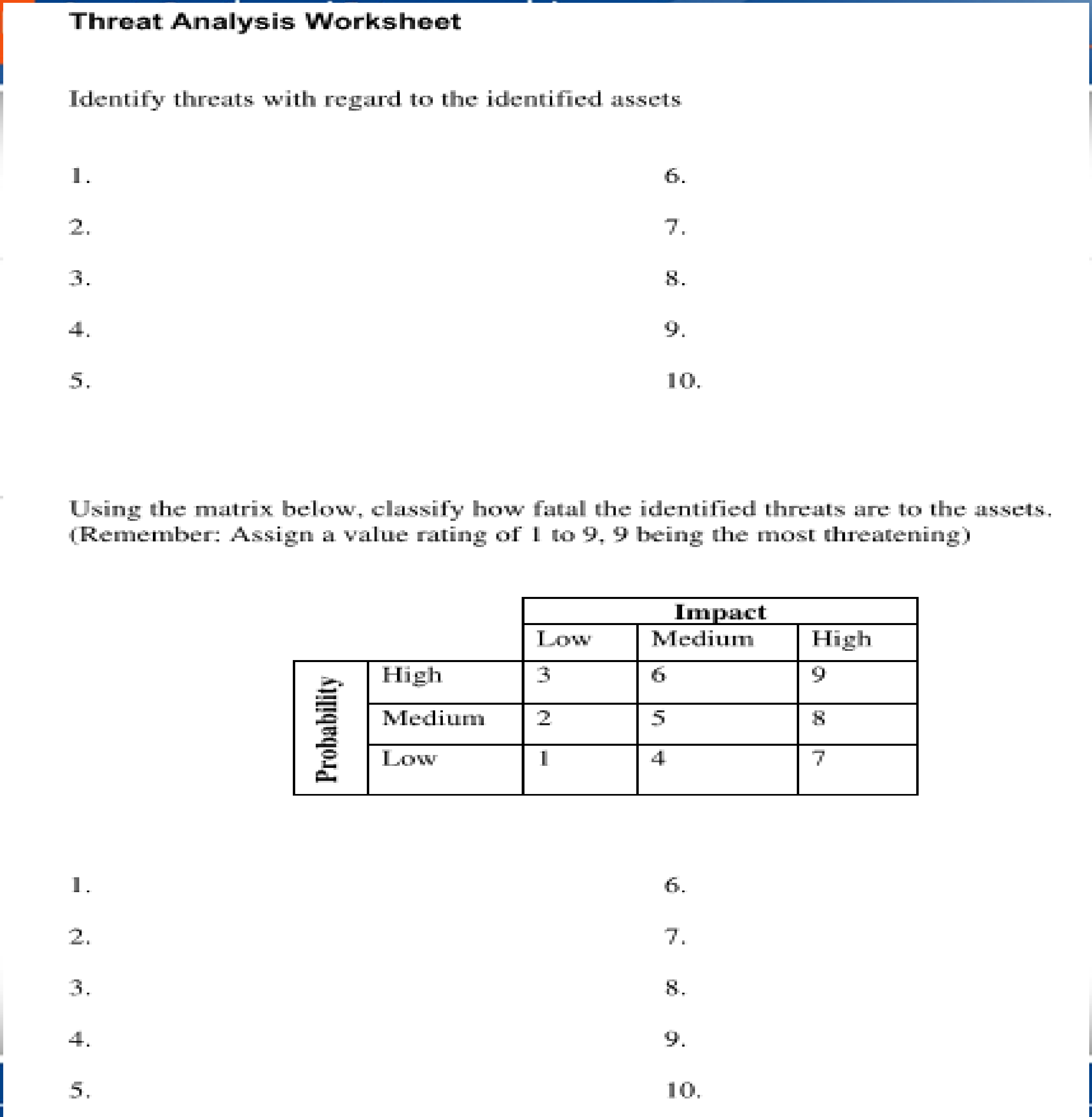
Asset Analysis Worksheet

Identify assets within your organization (i.e. databases, computers, etc…)

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Identify how valuable the identified assets are to the organization.
(Remember: Assign a value rating of 1 to 5, 5 being the most valuable)

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.



Threat Analysis Worksheet

Identify threats with regard to the identified assets

1.

2.

3.

4.

5.

6.

7.

8.

9.

10.

Using the matrix below, classify how fatal the identified threats are to the assets. (Remember: Assign a value rating of 1 to 9, 9 being the most threatening)

		Impact		
		Low	Medium	High
Probability	High	3	6	9
	Medium	2	5	8
	Low	1	4	7

1.

2.

3.

4.

5.

6.

7.

8.

9.

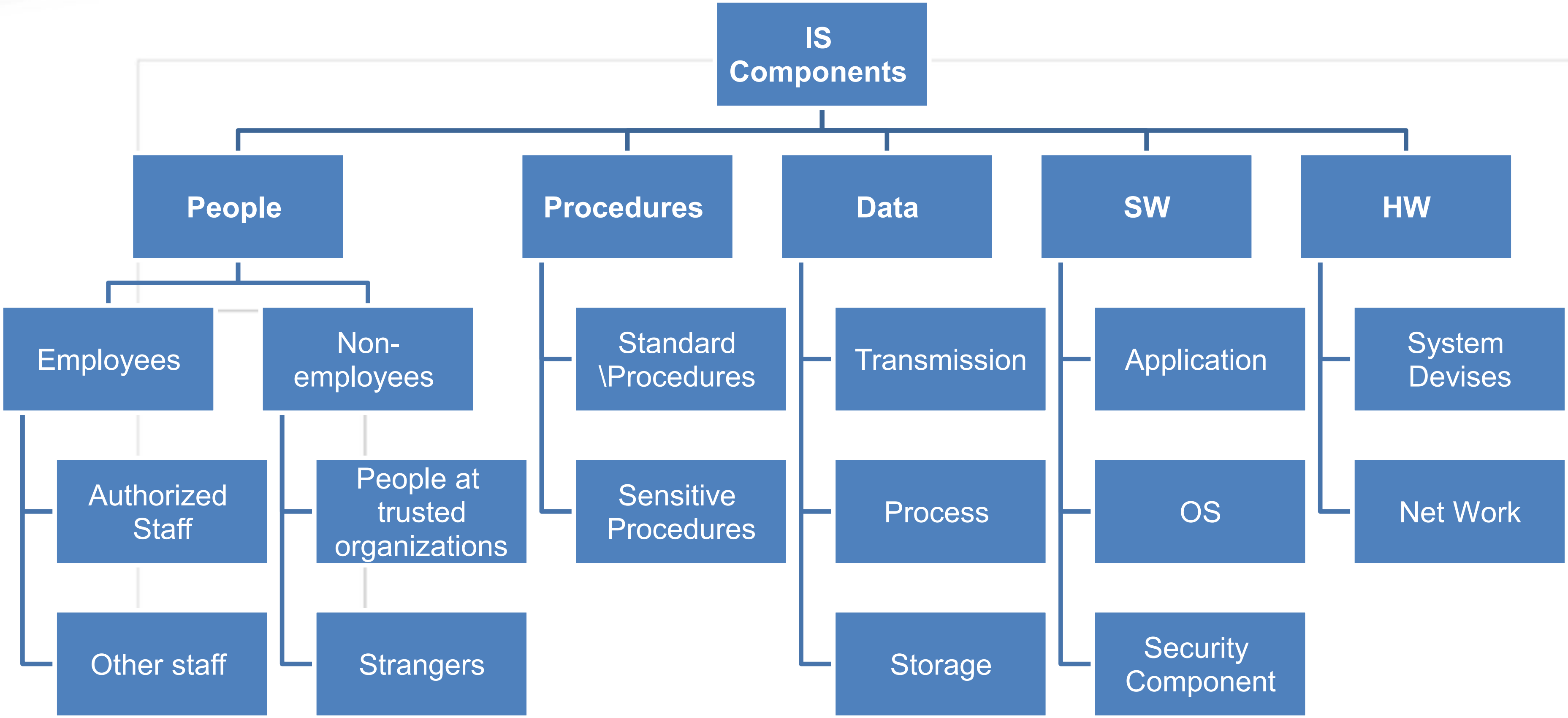
10.

Identifying Assets and Threats

Assignment

- Design matrices to summary them.

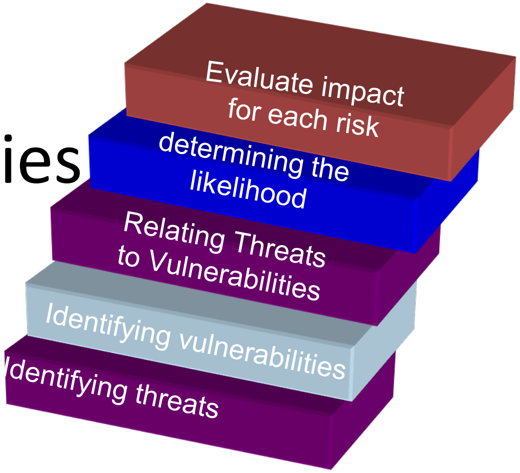
Information Assets



How to assess the risks

Risk is assessed by following the following steps:

1. Identifiying assets
2. Identifying threats and impact
3. Identifying vulnerabilities
4. Relating Threats to Vulnerabilities
5. determining the likelihood
6. Evaluate impact for each risk


Evaluate impact for each risk
determining the likelihood
Relating Threats to Vulnerabilities
Identifying vulnerabilities
Identifying threats

Reference

- Information Security Risk Analysis, Peltier
- Sanjay Goel, School of Business/Center for Information Forensics and Assurance, University at Albany Proprietary Information