QS STARS RATED FOR EXCELLENCE 2012

FPT Education

FPT UNIVERSITY

ĐẠI HỌC FPT CẦN THƠ

Risk Management Fundamentals

cantho.fpt.edu.vn

Objectives

- Concepts associated with Risk Management
- Components of Risk
- Importance of Risk Management
- Risk Identification
- Risk Management Techniques

What Is Risk?

- Risk is the likelihood that a loss will occur
- Losses occur when a threat exposes a vulnerability
- Major vs. minor risks
- Profitability vs. survivability

Basic Concepts

Asset

- Information, property, people or anything else that we care about

Threat

- A potential form of loss or damage; many threats are only potential threats, but we plan for them because they might happen

Threat agent

- A vector for the threat, a way for the threat to occur; could be a person, an event, or a program running an attack

Vulnerability

- A weak spot where an attack is more likely to succeed

Exploit

- A method of attack

Basic Concepts (cont.)

Incident

- A threat that has actually become a reality, an event that is or has caused loss to our organization

Probability of occurrence

- The odds that a particular threat will exploit a particular vulnerability successfully

Impact

- The kind (e.g. money, productivity, customer confidence) and scale (usually expressed in dollars) of loss that an occurrence would have on an organization; a high score here means we should concentrate some of our limited budget on protecting a particular asset

Basic Concepts (cont.)

Risk

- A more formal definition of risk uses some of the terms above: *Risk* is the probability that a particular threat will exploit a vulnerability causing harm to an organization.

Control

- A process that we put in place to reduce the impact and/or probability of a risk

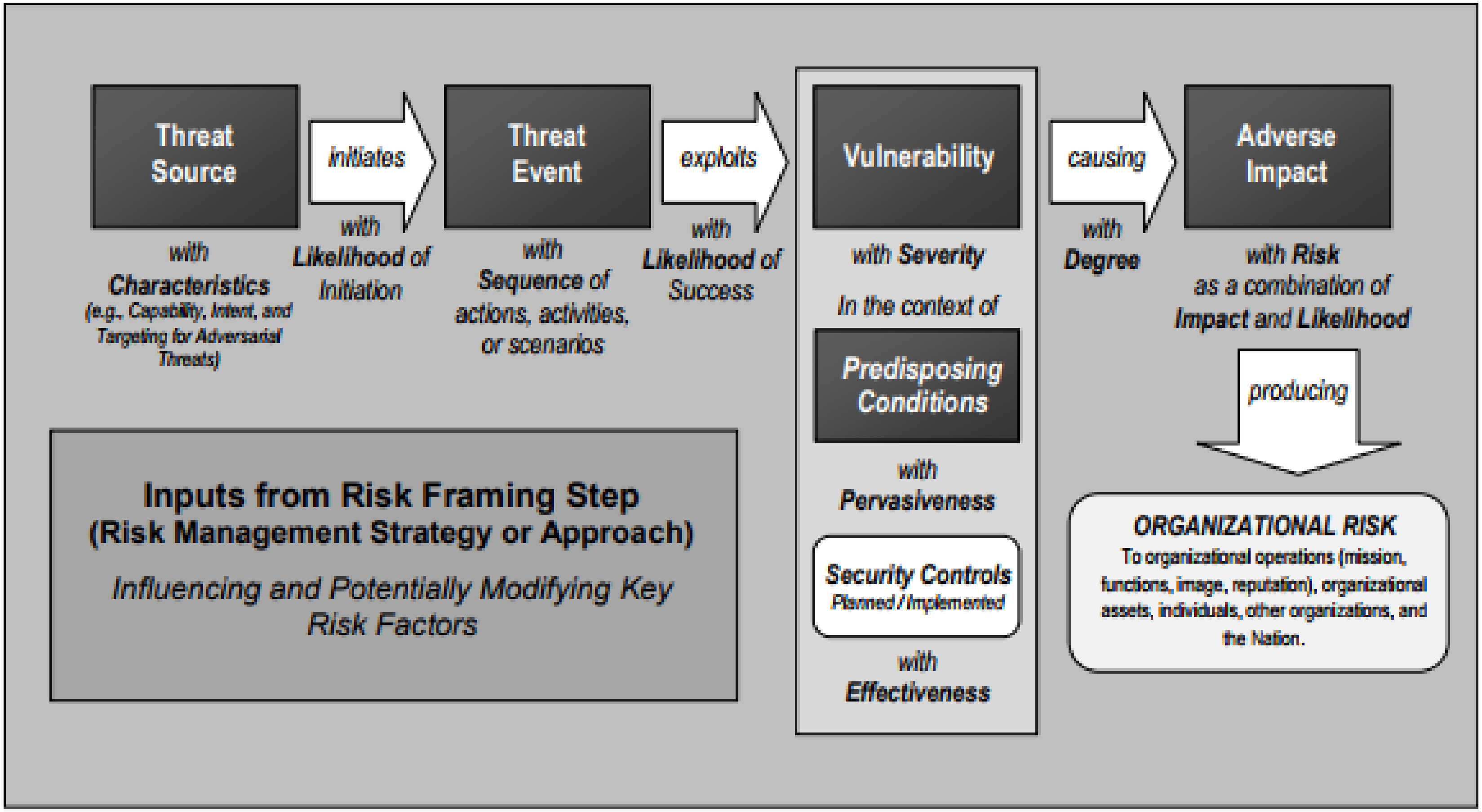
Policy

- a plan that influences decisions;
- a guiding principle for decisions and actions;
- a set of rules about what actions are acceptable and what actions are unacceptable

FPT Education

FPT UNIVERSITY

Generic Risk Model with Key Risk Factors



Threat Source

initiates

with Likelihood of Initiation

Threat Event

exploits

with Likelihood of Success

Vulnerability

causing

with Degree

Adverse Impact

with Characteristics (e.g., Capability, Intent, and Targeting for Adversarial Threats)

with Sequence of actions, activities, or scenarios

with Severity

In the context of

Predisposing Conditions

with Pervasiveness

Security Controls Planned / Implemented

with Effectiveness

with Risk as a combination of Impact and Likelihood

producing

ORGANIZATIONAL RISK

To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

Inputs from Risk Framing Step (Risk Management Strategy or Approach)

Influencing and Potentially Modifying Key Risk Factors

Compromised Business Functions and Assets

Two value types:

- *Tangible*
- *Intangible*

Assets themselves can be classified as

- *Tangible* (physical assets, including data and intellectual property). or
- *Intangible* (reputation, service ratings, customer loyalty, service to prestigious customers).

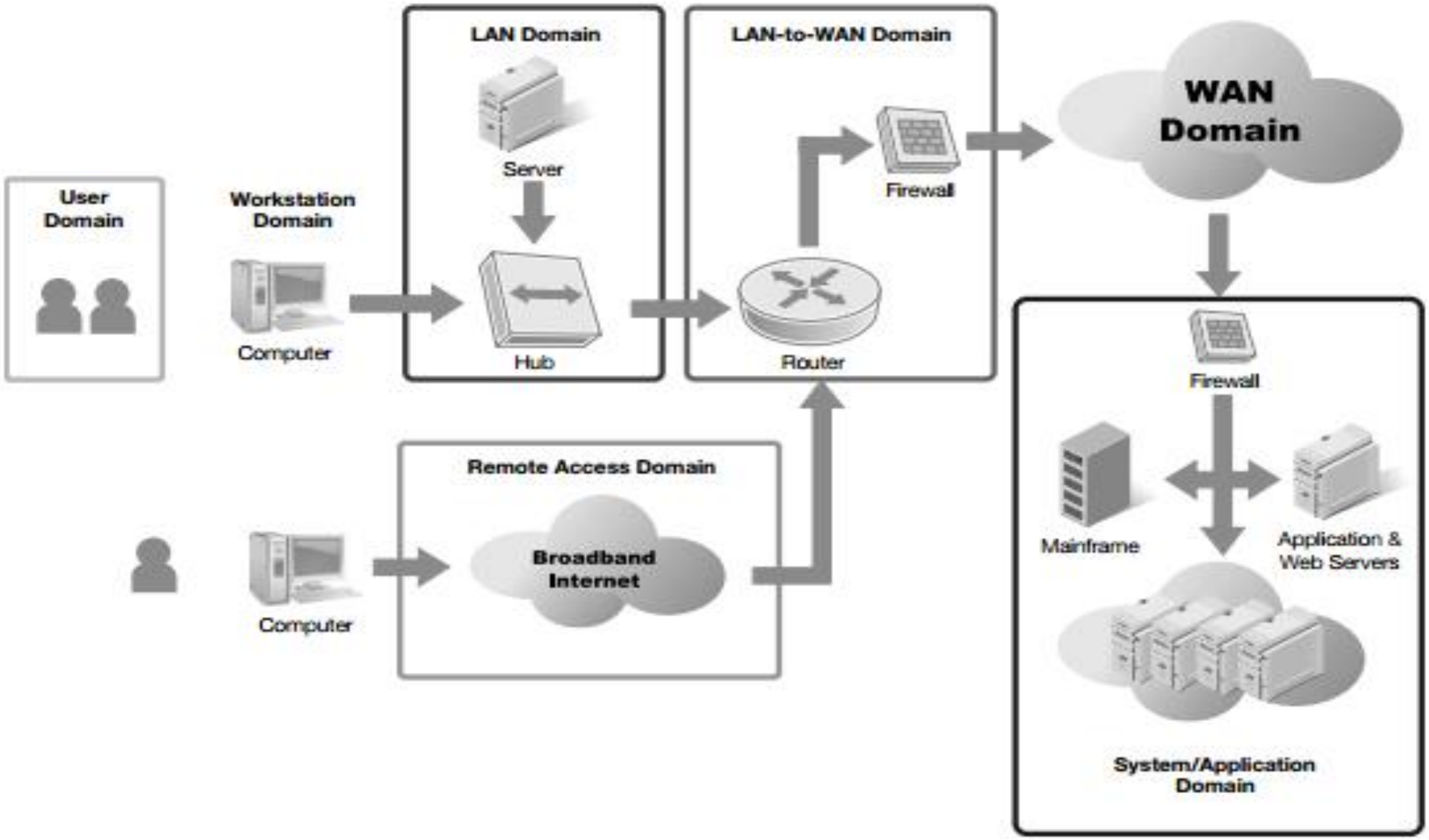
Driver of Business Costs

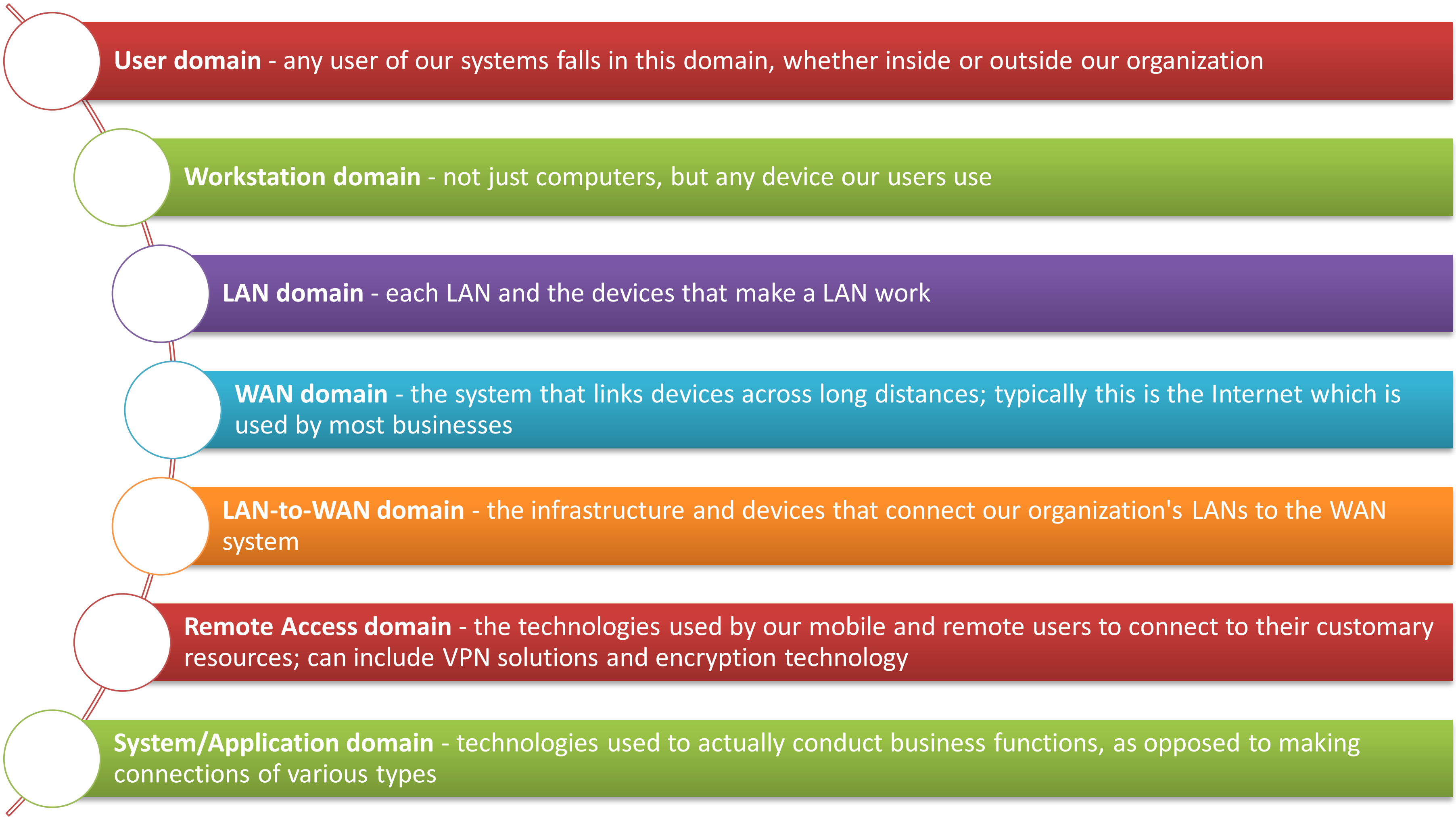
- After risks are identified, steps can be taken to reduce or manage the risk:
  - Risks are often managed by implementing *countermeasures* or *controls*.
  - The costs of managing risk need to be considered in total business costs.
- Profitability - revenues minus costs.
- Survivability - The ability of a company to survive loss due to a risk.
- Out-of-pocket-cost - the cost to reduce a risk with a particular control.

Driver of Business Costs

- Lost opportunity cost - Money spent to reduce risks can’t be spent elsewhere.
- Future cost - the cost to maintain the control over time, which may come from licensing, subscription, or maintenance of a system.
- Client/stakeholder confidence - think of this as related to customer good will, which can be lost if our organization has a documented loss due to an attack.

Major Components of Risk to an IT Infrastructure





User domain - any user of our systems falls in this domain, whether inside or outside our organization

Workstation domain - not just computers, but any device our users use

LAN domain - each LAN and the devices that make a LAN work

WAN domain - the system that links devices across long distances; typically this is the Internet which is used by most businesses

LAN-to-WAN domain - the infrastructure and devices that connect our organization's LANs to the WAN system

Remote Access domain - the technologies used by our mobile and remote users to connect to their customary resources; can include VPN solutions and encryption technology

System/Application domain - technologies used to actually conduct business functions, as opposed to making connections of various types

Threats, Vulnerabilities and Impact

Threat is any circumstance or event with the potential to cause a loss

Vulnerability is a weakness

The impact identifies the severity of the loss

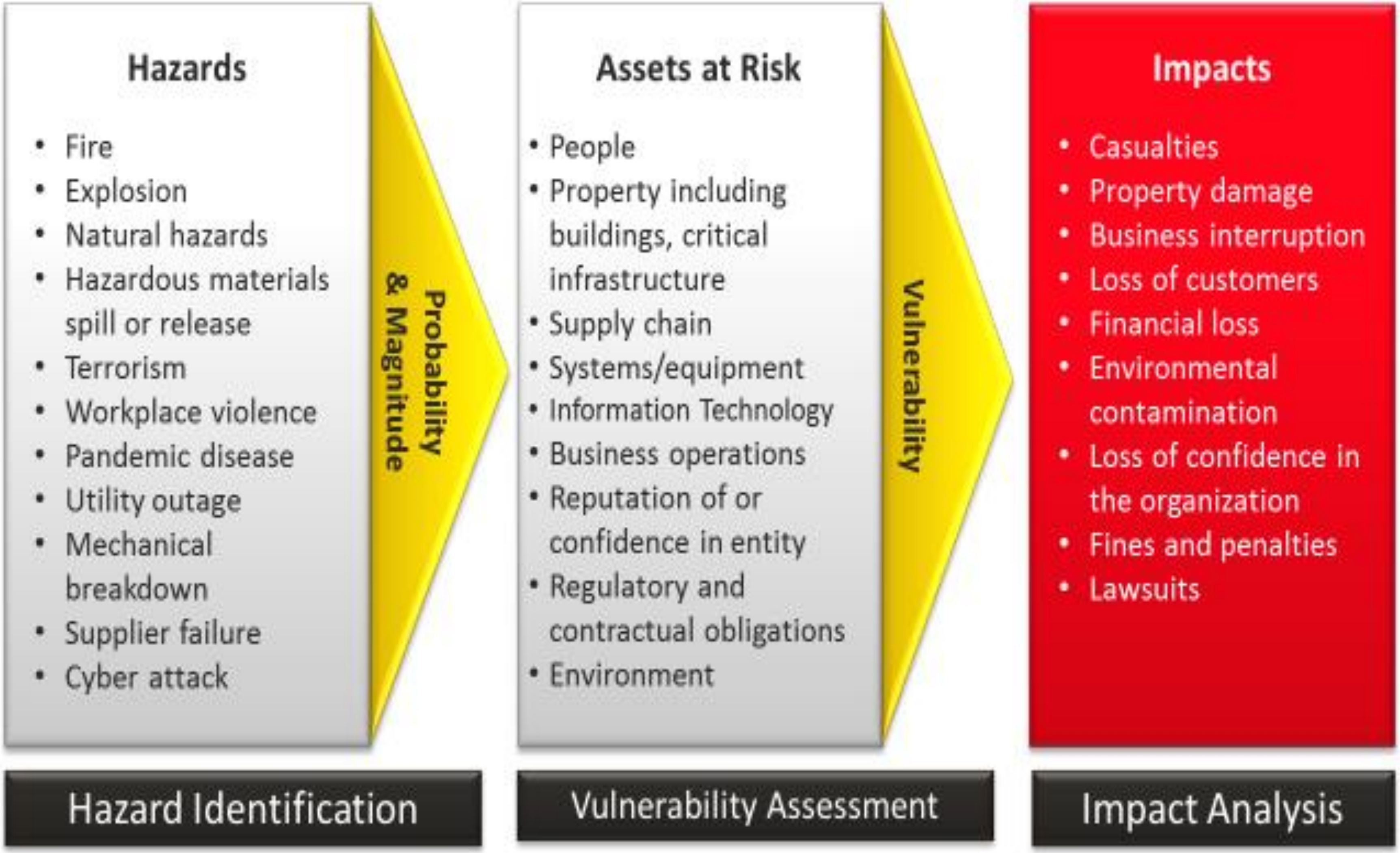
Threats are attempts to exploit vulnerabilities that result in the loss of confidentiality, integrity, or availability of a business asset (The C-I-A triad).

Threats, Vulnerabilities and Impact

The severity of a an attack's impact:

- ***very low*** - negligible adverse effect; the effects are small and not noticeable
- ***low*** - limited adverse effect; damage is minor and critical business functions are degraded
- ***moderate*** - serious adverse effect; damage may be significant and critical business functions are significantly degraded
- ***high*** - one severe or catastrophic effect; there may be major financial loss and and/or serious injury to staff
- ***very high*** - multiple severe or catastrophic effects; see above

Risk Assessment Process Diagram



Hazards

- Fire
- Explosion
- Natural hazards
- Hazardous materials spill or release
- Terrorism
- Workplace violence
- Pandemic disease
- Utility outage
- Mechanical breakdown
- Supplier failure
- Cyber attack

Probability & Magnitude

Assets at Risk

- People
- Property including buildings, critical infrastructure
- Supply chain
- Systems/equipment
- Information Technology
- Business operations
- Reputation of or confidence in entity
- Regulatory and contractual obligations
- Environment

Vulnerability

Impacts

- Casualties
- Property damage
- Business interruption
- Loss of customers
- Financial loss
- Environmental contamination
- Loss of confidence in the organization
- Fines and penalties
- Lawsuits

Hazard Identification

Vulnerability Assessment

Impact Analysis

Risk Management

Risk Management is the practice of identifying, assessing, controlling, and mitigating risks.

Threats and vulnerabilities are key drivers of risk.

Identifying the threats and vulnerabilities - an important step.

Risk Management attempts to identify the risks

that can be minimized and implement controls to do so.

Risk Management starts with a Risk Assessment (or Risk Analysis).

Elements of Risk Management

- Assessing risks
  - Identify assets, including IT assets
  - Identify and prioritize threats and vulnerabilities
  - Identify likelihood that each vulnerability will be successfully exploited by each threat: risks
  - Identify the impact of each risk
- Identifying risks to manage
- Selecting controls
- Implementing and testing controls
- Evaluating controls over time

Importance of Risk Management to the Organization

- Risk affects an organization’s survivability
- Reasonableness
- Balancing Risk and Cost
- Role-Based Perceptions of Risk
  - Balancing security and usability
  - Different perceptions of risk, varying according to a person's role in the organization:
    - Management
    - System administrator
    - Tier 1 administrator
    - Developer
    - End user

Balancing Risk and Cost

- A simplified method of assigning a score to a threat:
  - Assigning the threat a probability of occurring in percentage.
  - Assigning the asset a relative value on a scale of 1 to 100.
  - Multiplying the two values - getting a relative impact score.

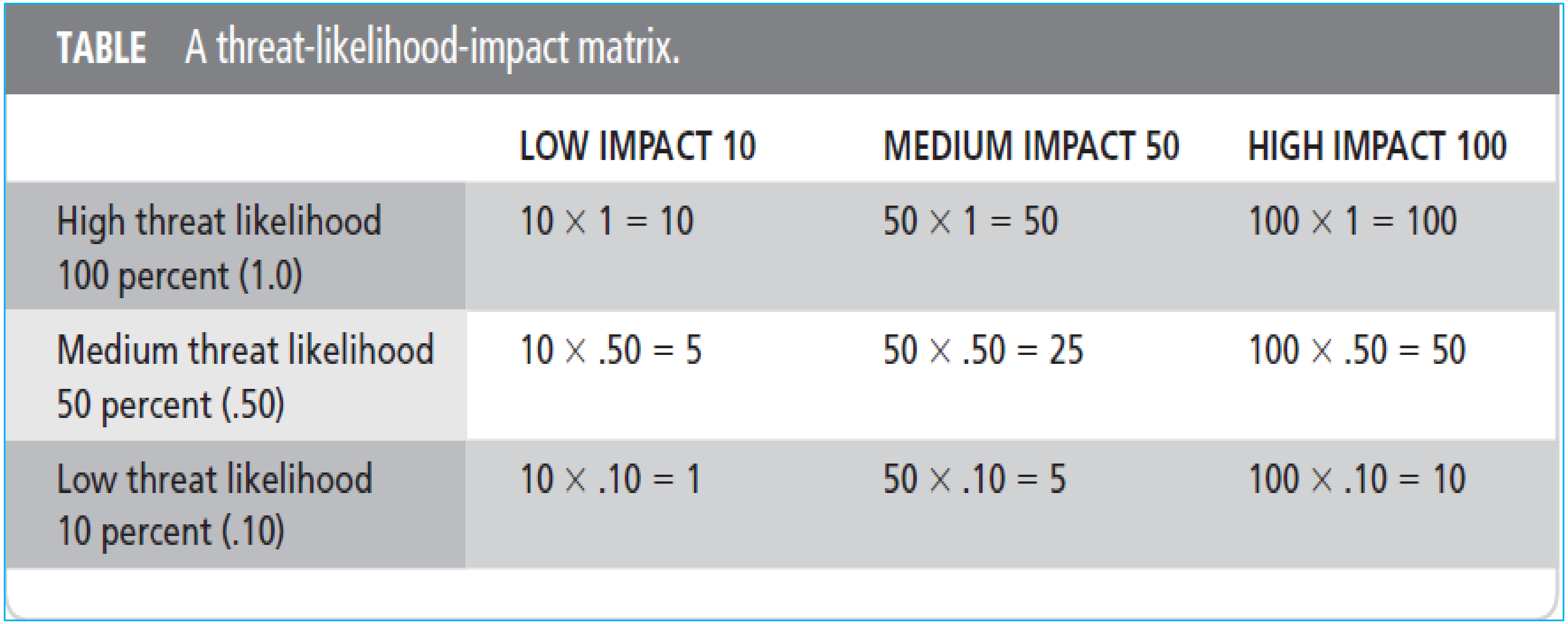


TABLE A threat-likelihood-impact matrix.

	LOW IMPACT 10	MEDIUM IMPACT 50	HIGH IMPACT 100
High threat likelihood 100 percent (1.0)	10 × 1 = 10	50 × 1 = 50	100 × 1 = 100
Medium threat likelihood 50 percent (.50)	10 × .50 = 5	50 × .50 = 25	100 × .50 = 50
Low threat likelihood 10 percent (.10)	10 × .10 = 1	50 × .10 = 5	100 × .10 = 10

Risk Identification Techniques

Identify threats

Identify vulnerabilities

Estimate the likelihood of a threat exploiting a vulnerability

Identifying Threats

- Loss of confidentiality
- Loss of integrity
- Loss of availability
- External or internal
- Natural or man-made
- Intentional or accidental

Threats: Examples

- An unauthorized employee trying to access data
- Any type of malware
- An attacker defacing a Web site
- Any DoS or DDoS attack
- An external attacker trying to access data
- Any loss of data
- Any loss of services

Threats: Examples (cont.)

- A social engineer tricking an employee into revealing a secret
- Earthquakes, floods, or hurricanes
- A lightning strike
- Electrical, heating, or air conditioning outages
- Fires

Identifying Vulnerabilities

- A short list of sources of information telling us about vulnerabilities and attacks against them:
  - Audits
  - Certification and accreditation records
  - System logs
  - Prior events
  - Trouble reports
  - Incident response team records

Using the Seven Domains of a Typical IT Infrastructure to Identify Weaknesses

- **User Domain** - social engineering attacks begin with people, such as any of our system users
- **Workstation Domain** - computers that are not patched, and those whose antivirus or antimalware programs are not regularly updated are vulnerable
- **LAN Domain** - network data needs protection, typically with access controls as the first line of defense
- **WAN Domain** - this domain contains our public facing devices, such as our web servers, which are primary targets for attackers
- **LAN-to-WAN Domain** - this domain provides our users with access to the Internet, including all the dangers that lurk in it
- **Remote Access Domain** - remote users may be using their own equipment (e.g. storage media, smartphone, and personal computers), which may have been exposed to viruses and malware without the user knowing about it
- **System/Application Domain** - a common attack ploy is to inject SQL code into forms, web pages, and entry fields in programs that our users and customers are meant to use

Pairing Threats with Vulnerabilities

- Threats are matched to existing vulnerabilities to determine the likelihood of a risk.

$$\textit{Risk} = \textit{Threat} \times \textit{Vulnerability}$$

- Threat and vulnerability often don’t have numerical values.

$$\textit{Total Risk} = \textit{Threat} \times \textit{Vulnerability} \times \textit{Asset Value}$$

Risk Management Techniques

Major steps of Risk Management:

- Identifying risks
- Assessing risks
- Determining which risks will be handled and which risks will accepted
- Taking steps to reduce risk to an acceptable level.

Handling a risk:

- Avoidance
- Transference
- Mitigation
- Acceptance

Cost-Benefit Analysis (CBA)

- Performing a CBA to help determine which controls or countermeasures to implement.
- A CBA starts by gathering data to identify the costs of the controls:
  - *Cost of the control* - This includes the purchase costs plus the operational costs over the lifetime of the control.
  - *Projected benefits* - This includes the potential benefits gained from implementing the control. You identify these benefits by examining the costs of the loss and how much the loss will be reduced if the control is implemented.
- Some of the hidden costs may be:
  - Costs to train employees
  - Costs for ongoing maintenance
  - Software and hardware renewal costs

Residual Risk

- Residual risk - the risk that remains after applying controls.
- Taking steps to reduce the risk to an acceptable level:
  - The risk that's left is residual risk.

Residual Risk = Total Risk × Controls

Summary

- Risk occur when threats exploit vulnerabilities, resulting in a loss.
- The loss can compromise business functions and business assets.
- Risk management helps a company identify risks that need to be reduced.
- The first step in risk management are to identify threats and vulnerabilities.
- Four techniques for managing risk: avoided, transferred, mitigated, or accepted.
- Primary risk management technique is risk mitigation.

Summary

- Risk mitigation is also known as risk reduction or risk treatment.
- You reduce vulnerabilities by implementing controls.

Assessment

1. Which one of the following properly defines risk?
   a. Threat x Mitigation
   b. Vulnerability x Controls
   c. Controls x Residual Risk
   d. Threat x Vulnerability

Assessment

2. Which one of the following properly defines total risk?

   a. Threat - Mitigation

   b. Threat x Vulnerability x Asset Value

   c. Vulnerability - Controls.

   d. Vulnerability x Controls.

Assessment

3. What can you do to manage risk?

   a. Accept

   b. Transfer

   c. Avoid

   d. Migrate

THANK YOU!