SECURITY RISK MANAGEMENT AND ETHICS

MALEK AL ZABEN

ACADEMIC CONTENT DEPARTMENT

ERROR CATCHERS

TABLE OF CONTENT

CHAPTER ONE — INTRODUCTION TO SECURITY RISK MANAGEMENT 1 10

CHAPTER TWO — SECURITY RISK MANAGEMENT

CHAPTER THREE — SECURITY RISK ASSESSMENT

CHAPTER FOUR — IDENTIFYING AND ANALYZING THREATS, VULNERABILITIES, AND EXPLOITS

CHAPTER FIVE — DEVELOPING RISK MANAGEMENT PLAN

QUESTIONS — SUGGESTED AND PAST QUESTIONS

CHAPTER ONE

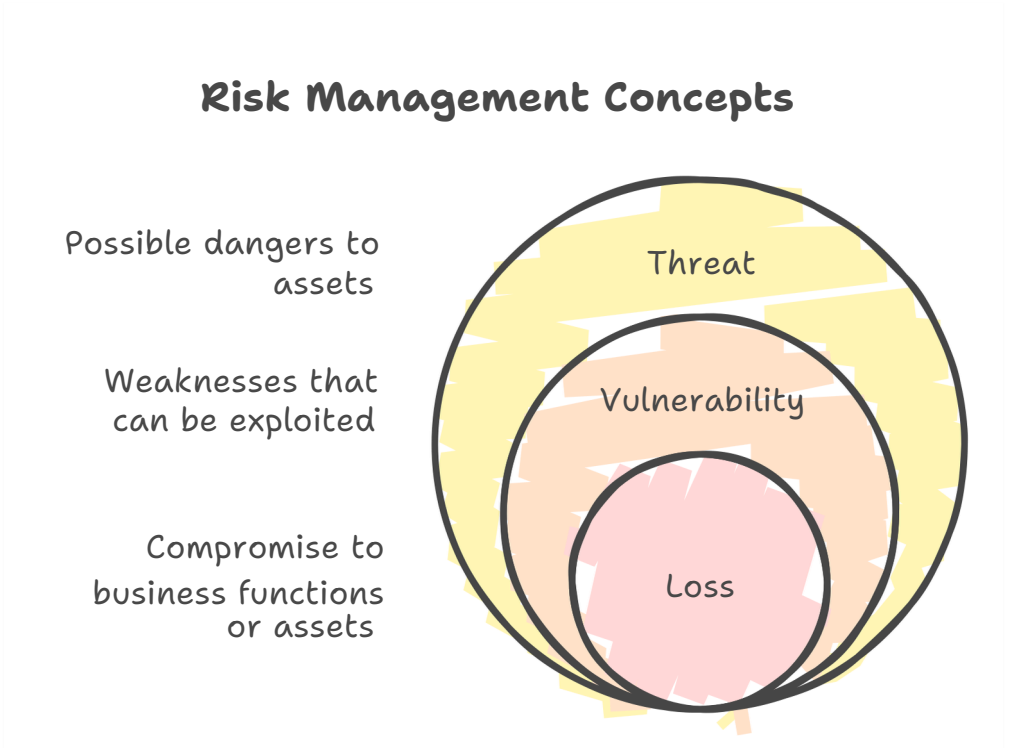
INTRODUCTION TO SECURITY RISK MANAGEMENT

INTRODUCTION TO SECURITY RISK MANAGEMENT

Risk : Risk refers to the likelihood of a loss occurring when a threat exploits a vulnerability. Businesses face different levels of risks, ranging from minor to severe. risk management techniques involve identifying and prioritizing risks, enabling administrators and managers intelligently decide what to do about any type of risk. The decisions is about whether to avoid, transfer, mitigate, or accept them. The common themes of these definitions are threat, vulnerability, and loss.

The most important definitions in this chapter :

- Threat: activity that represents a possible danger [Any potential danger].
- Vulnerability: Is a weakness.
- Loss: results in a compromise to business functions or assets. [A negative impact on business functions or assets].



The overall goal is to reduce the losses that can occur from risk.

Business Losses:

1. Business Functions: The activities a business performs to provide services [Risks to business operations] , such as website failure or data loss, can affect revenue or decision-making.

2. Business Assets: Anything that has measurable value. Risks that impact both tangible assets (like computers, software, and data) and intangible assets (like customer confidence).

Tangible loss examples include lost revenue and repair costs, while intangible losses can include lost customers and future revenue.

One of the early steps in risk management is associated with identifying the assets of a company and their associated costs.

This data is used to prioritize risks for different assets

Once a risk is prioritized, it becomes easier to identify risk management processes to protect the asset.

3. Drivers of Business Costs: Managing risk can incur costs, including out-of-pocket expenses, lost opportunities, and future costs for ongoing security.

To prevent reducing profitability or not protecting the business, it's essential to strike the right balance.

Risks are often managed by implementing controls or countermeasures .

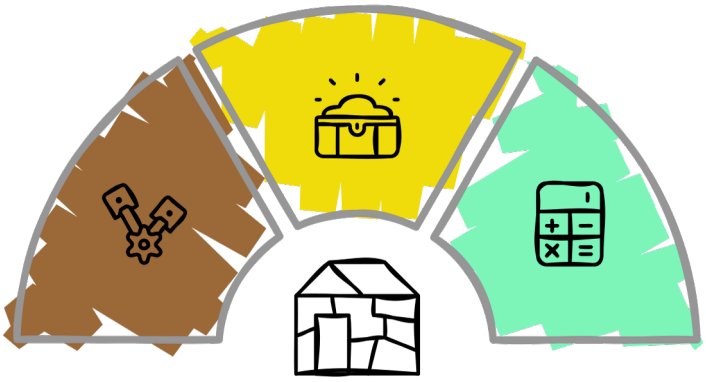
Business Losses

Business Assets

Impact on tangible and intangible assets

Business Functions

Risks to operations affecting revenue and decision-making



Drivers of Costs

Costs associated with managing risks and maintaining profitability [the right balance]

Profitability vs. Survivability:

- **Profitability:** A company's ability to generate profit, which can be threatened by losses

. Profitability = revenues - costs.

- **Survivability:** A company's ability to continue operating even in the face of losses, Both profitability and survivability must be considered when considering risk to ensure a business can continue its operations while minimizing potential losses.

Consider the following items is important when considering profitability and survivability.

1- Out-of-pocket costs—The cost to reduce risks comes from existing funds.

2- Lost opportunity costs—Money spent to reduce risks can't be spent elsewhere. This may result in lost opportunities if the money could be used for some other purpose.

3- Future costs—Some countermeasures require ongoing or future costs. These costs could be for renewing hardware or software. Future costs can also include the cost of employees to implement the countermeasures.

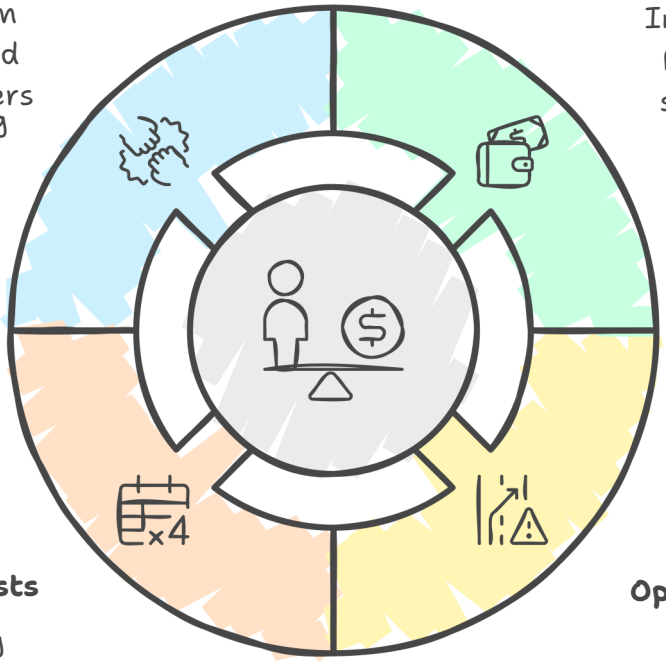
4- Client/stakeholder confidence—The value of client and stakeholder confidence is also important. If risks aren't addressed, clients or stakeholders may lose confidence when a threat exploits a vulnerability, resulting in a significant loss to the company.

Balancing Profitability and Survivability

"Consider the following items"

Stakeholder Confidence
Trust from clients and stakeholders impacting business stability

Out-of-Pocket Costs
Immediate financial spending



Future Costs
Ongoing expenses for maintaining and updating risk countermeasures

Lost Opportunity Costs
spent to reduce risks can't be spent elsewhere

A weakness in any one of the domains can be exploited by an attacker even if the other six domains have no vulnerabilities

The Seven Domains of IT Infrastructure and Associated Risks:

1. User Domain: Risks from human error or social engineering . (weak passwords, phishing , etc). People are often the weakest link in IT security.

Users may **unknowingly** bring viruses from home via universal serial bus (USB) thumb drives

2. Workstation Domain: Risks to end-user computers, workstation Domain is susceptible to these vulnerabilities [malware and unpatched software vulnerabilities , antivirus software isn't installed , bugs and vulnerabilities , software vendors {if they don't release patches and fixes }] . 2. some malwares can releases worm components that can spread across the network.

3. LAN Domain: Risks within the internal network [the area that is inside the firewall].

if each individual device on the network not protected all devices at risk ,the internal LAN is considered as a trusted zone.

sniffing attack occur when an attacker uses a protocol analyzer to capture data packets.

protocol analyzer [sniffer] : An experienced attacker can read the actual data within these packets .

If we used switches instead of hubs the probability of the sniffing attack is decrease, because the attacker must have physical access to the switch to capture the data such as data sniffing or unprotected network devices

4. LAN-to-WAN Domain: The local area network to the wide area network ,WAN Domain is considered an untrusted zone Why ??

1- it is not controlled

2- accessible by attackers.

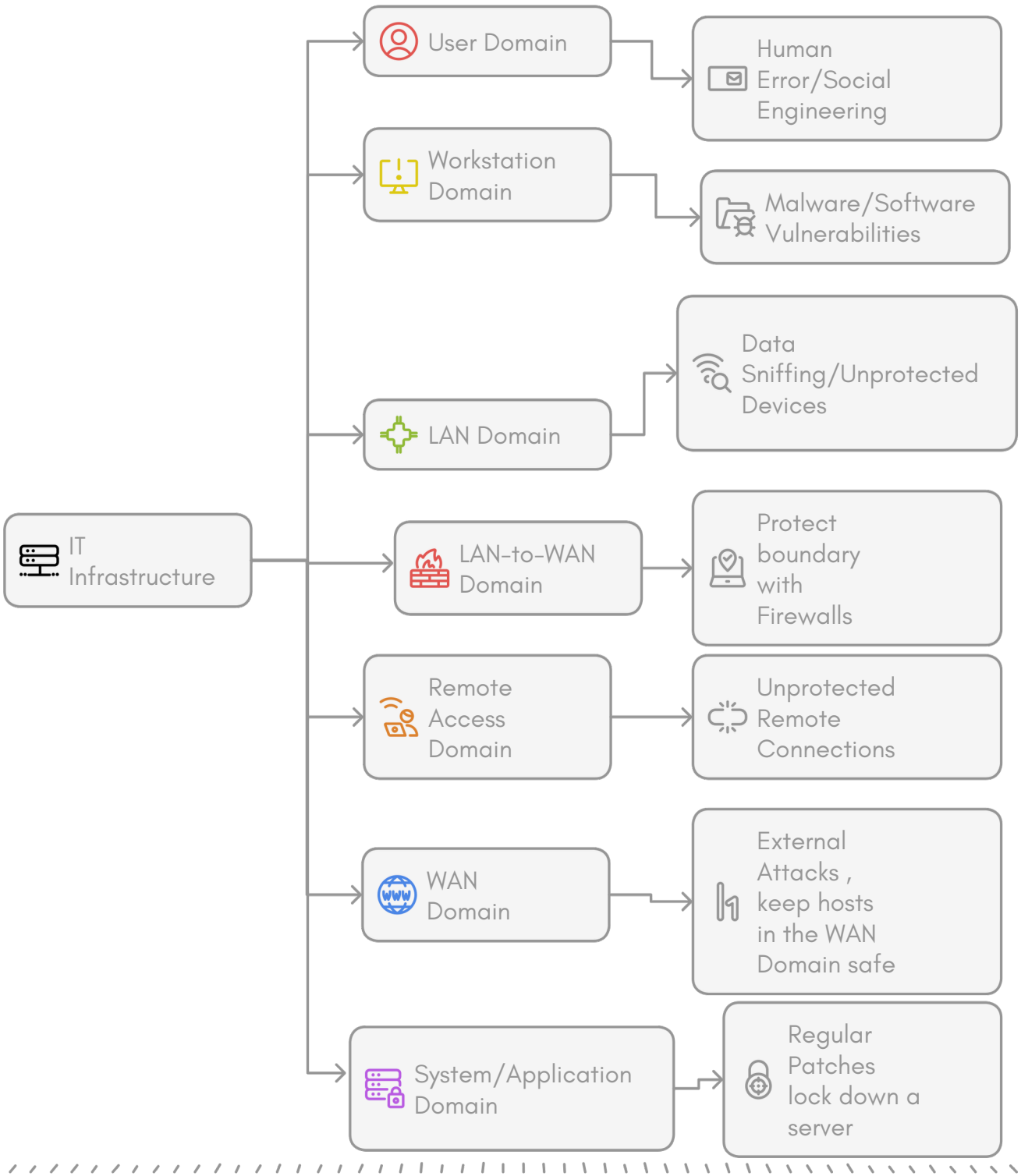
The area between the LAN and WAN zones firewalls are crucial for protection . This is also called the boundary, or the edge, we should protect the boundary [edge].

the high level of security is required to keep the LAN to WAN Domain safe.

6. WAN Domain: External networks like the internet, which are susceptible to attacks and require strong security measures. a business can also lease semiprivate lines from private telecommunications companies Semiprivate lines aren't as easily accessible as the Internet
A significant amount of security is required to keep hosts in the WAN Domain safe

7. System/Application Domain: Risks to servers and applications that support critical business functions, including the need for regular patches and strong access control. one of the problems with servers in the System/Application people tend to focus on areas of specialty [knowledge becomes specialized].
best practices to protect System/Application Domain : Remove unneeded services and protocols. Change default passwords Regularly patch and update the server systems. Enable local firewalls
Domain Name System (DNS) servers provide names to IP addresses for clients.
NOTE: You should lock down a server using the specific security requirements needed by the hosted application. An e-mail server requires one set of protections while a database server requires a different set

5. Remote Access Domain: Risks related to remote work, especially unprotected connections like VPNs .
Vulnerabilities of the VPN connection :
1- authentication is when the user provides credentials to prove identity If these credentials can be discovered, the attacker can later use them to impersonate the user.
2-when data is passed between the user and the server If the data is sent in clear text, an attacker can capture and read the data.
VPN connections use **tunneling protocols** to reduce the risk of data being captured 5. tunneling protocol will encrypt the traffic sent over the network the idea of tunneling protocol is to make it more difficult for attackers to capture and read data


IT Infrastructure
User Domain
Human Error/Social Engineering
Workstation Domain
Malware/Software Vulnerabilities
LAN Domain
Data Sniffing/Unprotected Devices
LAN-to-WAN Domain
Protect boundary with Firewalls
Remote Access Domain
Unprotected Remote Connections
WAN Domain
External Attacks , keep hosts in the WAN Domain safe
System/Application Domain
Regular Patches lock down a server

Threats, Vulnerabilities, and Impacts:

• Threats are events or activities that pose potential dangers, while **vulnerabilities** are weaknesses that allow threats to cause harm.

Threats are attempts to exploit vulnerabilities that result in the loss of confidentiality, integrity, or availability of a business asset.

• **Impact** describes the severity of loss, which can be categorized as high, medium, or low, depending on the consequences (financial loss, reputational damage, or human injury).

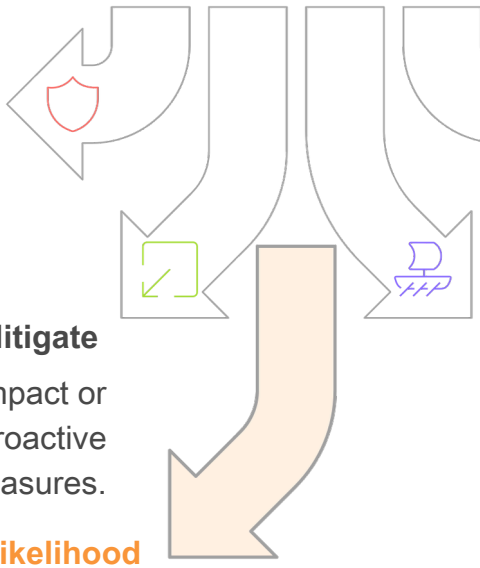
If any side of the triangle is breached or fails, security fails.

risks to confidentiality, integrity, or availability represent potential loss to an organization. Because of this, a significant amount of risk management is focused on protecting these resources

Confidentiality—Preventing unauthorized disclosure of information.
Integrity—Ensuring data or an IT system is not modified or destroyed.
Availability—Ensuring data and services are available when needed.

IT Security Management: Effective IT security management is essential for protecting business assets and data. It includes setting organizational security objectives, identifying threats, analyzing risks, and implementing safeguards. Regular monitoring, security awareness programs, and incident response are crucial for maintaining a secure IT environment.

Risk Treatment Alternatives



Avoid

Eliminates the risk by not proceed the activity that creates it.

Transfer

Shifts the risk to another party, often through insurance.

Mitigate

Reduces the risk's impact or likelihood through proactive measures.

Accept

accept the risk without taking further action, often for minor risks.

Reduce likelihood

implement suitable controls

CHAPTER TWO

SECURITY RISK MANAGEMENT

Definition and Importance of Risk Management

- **Risk Management** involves identifying ,assessing ,controlling ,and mitigating risks ,with the goal of minimizing potential losses while accepting that complete elimination of risks is impractical.
- Key drivers of risk are **threats** (external or internal events with potential harm) and vulnerabilities (weaknesses that threats can exploit).
- risk management isn't intended to be risk elimination
- risks that can be minimized and implement controls

Elements of Risk Management

1.RiskAssessment:

- Identify IT assets (etc ,data ,hardware) and their value.
- Identify threats and vulnerabilities to these assets . Prioritize the threats and vulnerabilities.
- Identify the likelihood a vulnerability will bee xploited by athreat. These are your risks.
- Identify the impact of a risk. Risks with higher impacts should be addressed first

2.Risk Identification:

- Risks can be managed by avoiding, transferring ,mitigating ,or accepting them.
- Selecting appropriate controls (countermeasures) focuses on reducing vulnerabilities.
- The decision is often based on the likelihood of the risk occurring, and the impact it will have if it occurs

3. Selection of controls

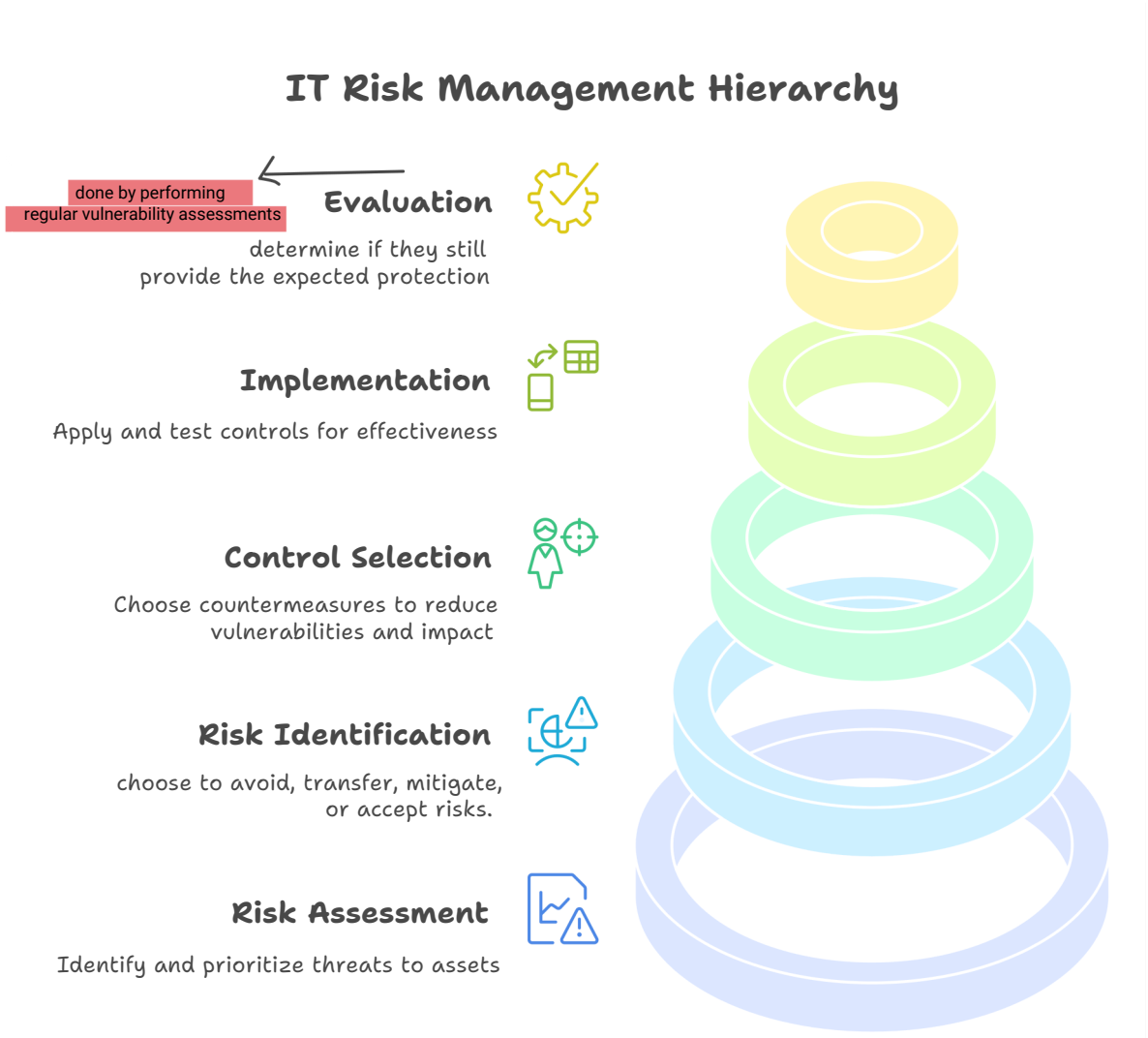
Control methods are also referred to as countermeasures. Controls are primarily focused on reducing vulnerabilities and impact

4. Implementation and Testing:

- Implementation and testing of controls—Once the controls are implemented ,you can test them to ensure they provide the expected protection.

5. Evaluation:

- Risk management is an ongoing process. You should regularly evaluate implemented controls to determine if they still provide the expected protection.
- Evaluation is often done by performing regular vulnerability assessments.



Role-Based Risk Perceptions

- One of the challenges with effective risk management is achieving a proper balance between security and usability.

- **Risk perspectives by role:**

- **Management:**

- Balances profitability and survivability and risk mitigation costs Management needs accurate facts to make decisions on which controls to implement to protect company assets.

- **System Administrators:**

- responsible for protecting the IT systems Focuses on locking down systems but may overlook usability.

- **Tier 1 administrator:**

- first line of defense for IT support, more concerned with usability than security or profitability they have limited administrative permissions.

- **Developers:**

- secure computing mindset developers They realize that security needs to be included from the design stage all the way to the release stage, developers haven't a security mindset, they try to patch security holes at the end of the development cycle.
  This patching mindset rarely addresses all problems, resulting in the release of vulnerable software.

- **End Users:**

- most concerned with usability, don't understand the reason for the security controls, try to break controls so they can complete their job.

Role-Based Risk Perceptions

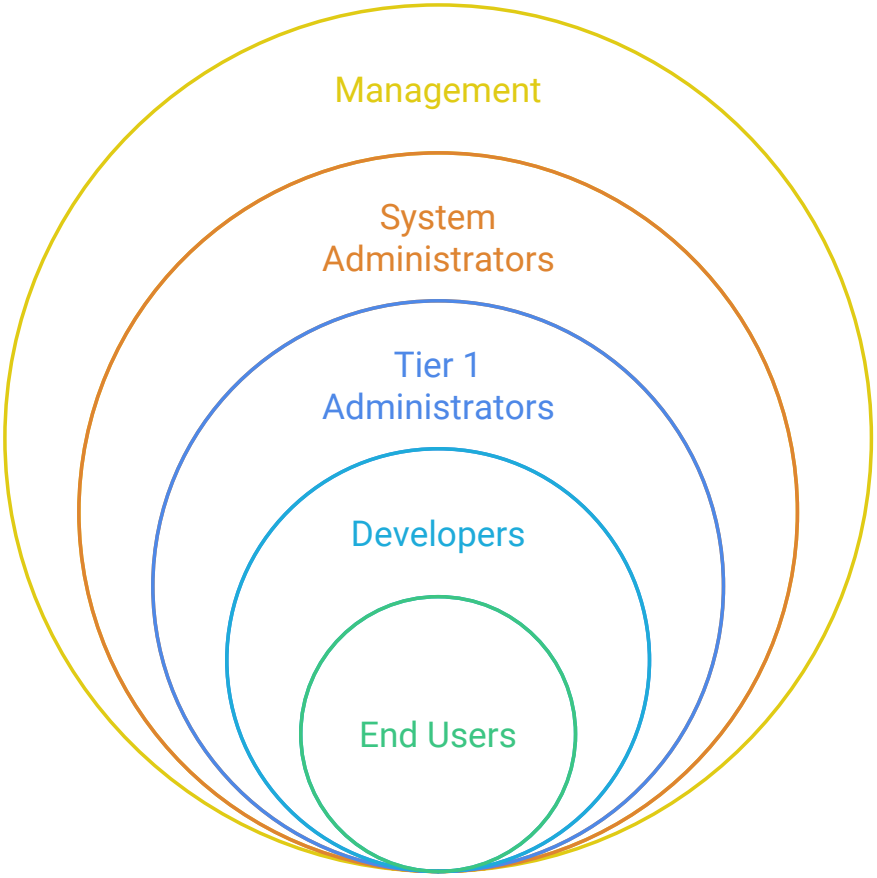
Balance profitability and risk mitigation

Focus on system protection

Balance usability with limited security

secure computing mindset developers or not

Prioritize usability over security



Risk Identification Techniques

- Identify Threats
- Identify vulnerabilities
- Estimate the likelihood

1. Threat identification: process of creating a list of threats. This list attempts to identify all the possible threats to an organization.

This is no small task. The list can be extensive.

Categories of threats:

- **External/Internal:**

External attackers outside the boundary of the organization can be risks that outside the control of the organization.

Internal threats are within the boundary of the organization related to employees or other personnel who have access to company resources.

- **Natural/Man-made:**

natural related to weather such as hurricane etc.

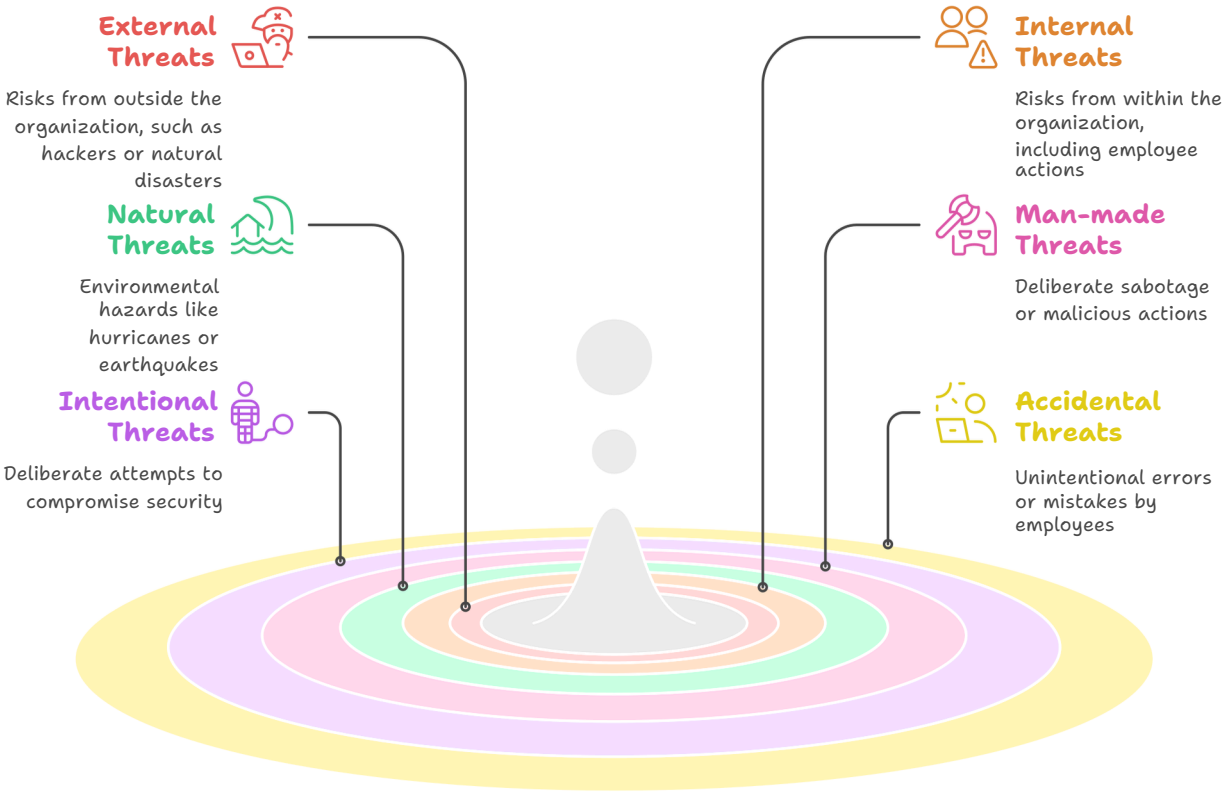
manmade threat is any threat from a person any attempt to sabotage resources.

- **Intentional/Accidental:**

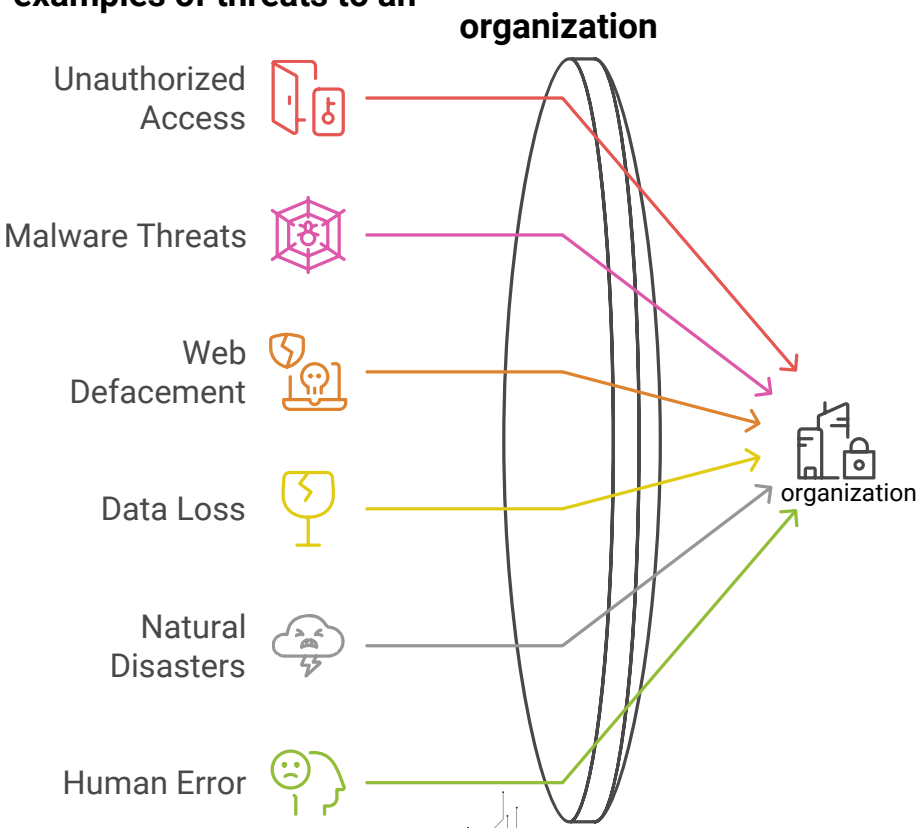
intentional is Any deliberate attempt to compromise confidentiality, integrity, or availability

accidental threats are Employee mistakes or user error, brainstorming session is method used to identify threats

Risk Identification Techniques



- **examples of threats to an organization**



2. Identifying Vulnerabilities: before threats occur, you'll have to dig a little to identify the weaknesses. Luckily, most organizations have a lot of sources which can help you.

1. System logs—Audit logs can determine if users are accessing sensitive data.
Firewall logs can identify traffic that is trying to breach the network and identify computers taken over by malware and acting as zombies.
DNS logs can identify unauthorized transfer of data.

2.Trouble reports— use databases to document trouble calls. These databases can contain a wealth of information.
With analysis, you can use them to identify trends and weaknesses.

3. Prior events—Previous security incidents are excellent sources of data , they help justify controls.
They show the problems that have occurred and can show trends.

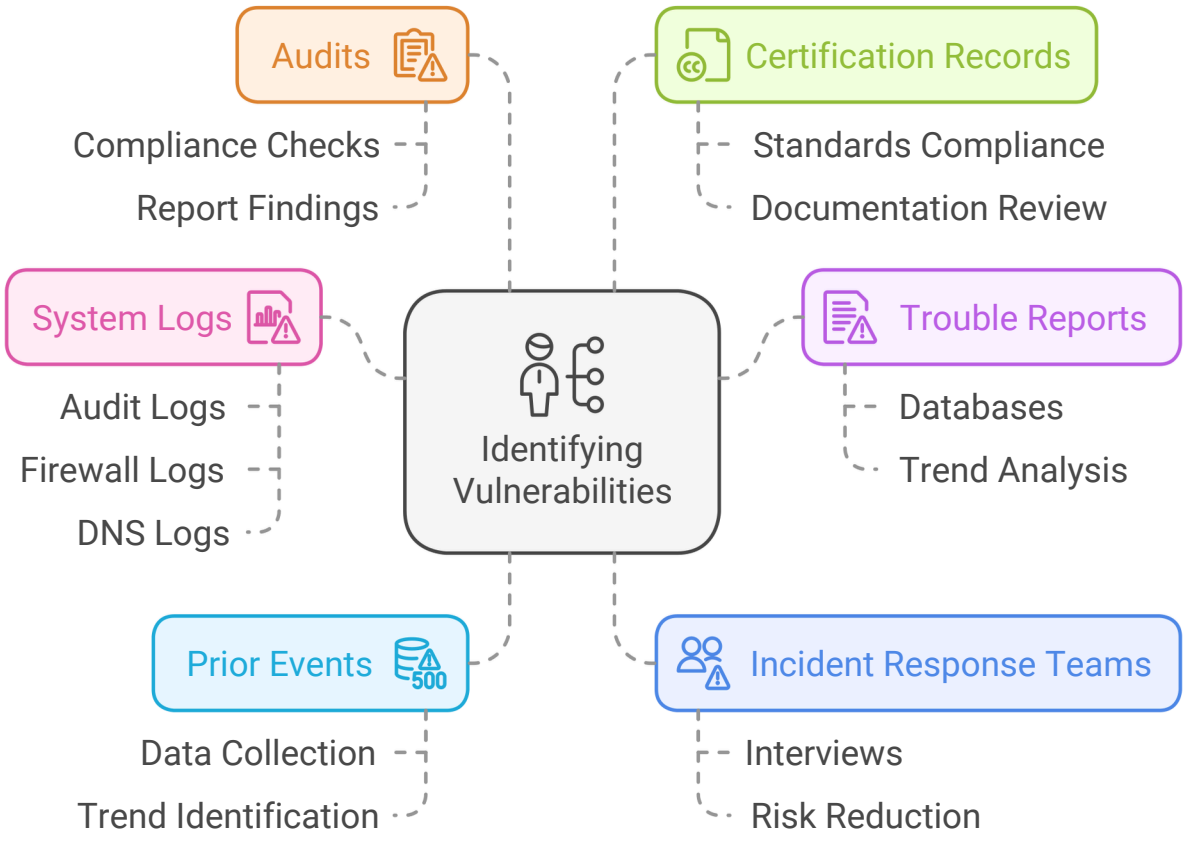
4. Incident response teams— These teams will investigate all the security incidents within the company.
These teams are often eager to help reduce risks. by interview team members and get a wealth of information.

5.Audits— Systems and processes are checked to verify a company complies with existing rules and laws.

At the completion of an audit, a report is created. These reports list findings which directly relate to weaknesses.

6. Certification and accreditation records— If the system meets the standards, the IT system can be accredited. The entire process includes detailed documentation.

This documentation can be reviewed to identify existing and potential weaknesses.



3. **Estimate the likelihood** of a threat exploiting a vulnerability Using the Seven Domains of a Typical IT Infrastructure.

(1) **User Domain**—Social engineering represents a big vulnerability.

(2) **Workstation Domain**—Computers that aren't patched can be exploited.

(3) **Lan Domain**—Any data on the network that is not secured with right "appropriate" access controls is vulnerable.

(4) **Lan-to-Wan Domain**— Firewalls with unnecessary ports open allow access to the internal network from the Internet that leads to make an unneeded vulnerability to visit malicious Web sites.

(5) **Wan Domain**—Any public-facing server is susceptible to DoS and DDoS attacks. A File Transfer Protocol (FTP) server that allows anonymous uploads can host malware "Warez" from black-hat hackers.

(6) **Remote access Domain**—Remote users may be infected with a virus but not know it. When they connect to the internal network via remote access, the virus can infect the network.

(7) **System/application Domain**—Database servers can be subject to SQL injection attacks. In a SQL injection attack, the attacker can read the entire database. SQL injection attacks can also modify data in the database.

- **Pairing Threats with Vulnerabilities**

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

Risk = Threat X Vulnerability

- **Risk Management Techniques**

Important to realize that risk management is not risk elimination.

The ultimate goal of risk management is to protect the organization.

Helps ensure a business can continue to operate and earn a profit.

- **Avoidance**

Eliminating the source of the risk—The company can stop the risky activity. Eliminating the exposure of assets to the risk—The company can move the asset

- **Transfer**

Shift risk responsibility, e.g., via insurance or outsourcing.

- **Mitigation**

reduce risk by reducing vulnerabilities the goal is not to eliminate the risk but instead, to make it too expensive for the attacker.

physical environment—Replace hubs with switches.

Change procedures—Implement a backup plan

Add fault tolerance Use failover clusters to protect servers

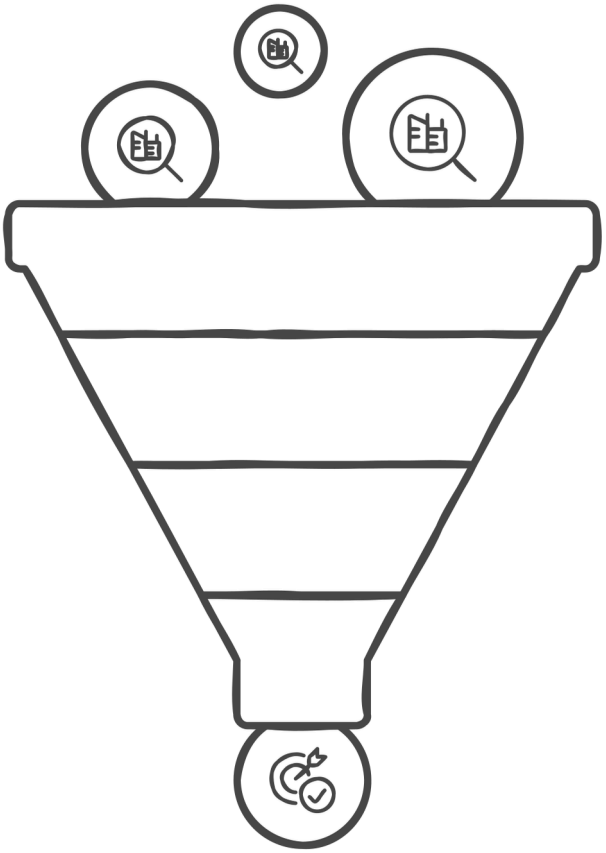
Modify the technical environment Use "IDS"

Train employees

- **Acceptance**

  Accept residual risks when mitigation costs exceed potential loss.This is commonly done when the cost of the control outweighs the potential loss.

The decision to accept a loss by evaluate the cost Using CBA



Risk Avoidance

Eliminating the source of the risk

Risk Transfer

Shifting risk responsibility

Risk Mitigation

Reducing vulnerabilities to risks

Risk Acceptance

Accepting residual risks

Cost-Benefit Analysis (CBA)

CBA starts by gathering data to identify the costs of the controls and benefits gained if they are implemented.

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.

hidden costs may be:

Costs to train employees.

Costs for ongoing maintenance Software and hardware renewal costs.

Evaluates the viability of risk controls by comparing their costs and benefits.

Helps in decisions like whether to implement, avoid, or transfer risks.

- **best practices to protect servers**

  Remove unneeded services and protocols.

  Change default passwords.

  Regularly patch and update the server systems.

  Enable local firewalls.

Note

If any side of the triangle is breached or fails, security fails.

Impact of Threat

Risks to confidentiality, integrity, and availability represent potential losses.

Impacts categorized as:

High: Major resource loss, harm to mission or reputation.

Medium: Costly resource loss or mission impediments.

Low: Minor resource loss or minor mission impact.

CHAPTER THREE

SECURITY RISK ASSESSMENT

soon ....

CHAPTER FOUR

IDENTIFYING AND ANALYZING THREATS, VULNERABILITIES, AND EXPLOITS

soon....

CHAPTER FOUR

IDENTIFYING AND ANALYZING THREATS, VULNERABILITIES, AND EXPLOITS

ERROR CATCHERS

WE CATCH WHAT OTHERS MISS !

MORE ABOUT US !