Chapter One: Introduction to Security Risk Management

Presented by:

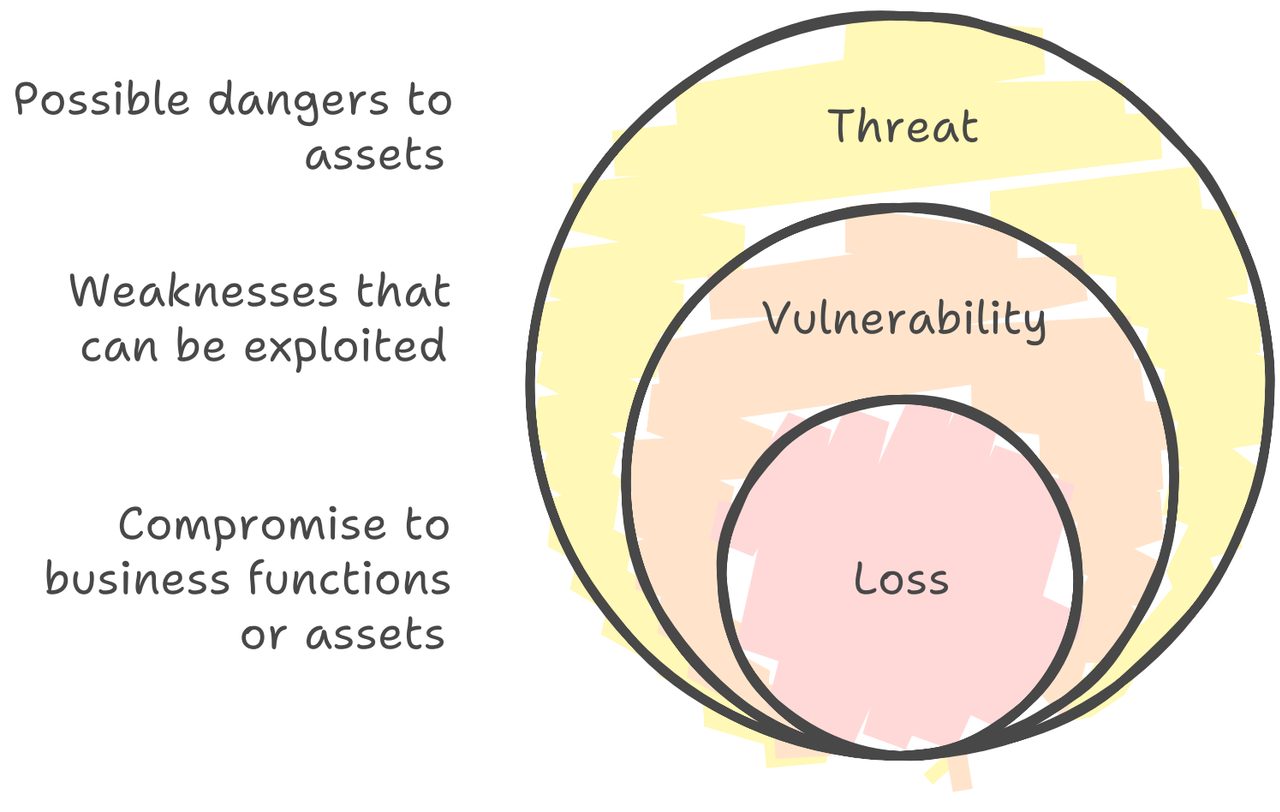
Malek Ahmad Al Zebn
B.Sc. STUDENT AT THE UNIVERSITY OF JORDAN

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].

Risk Management Concepts



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

Business Losses:

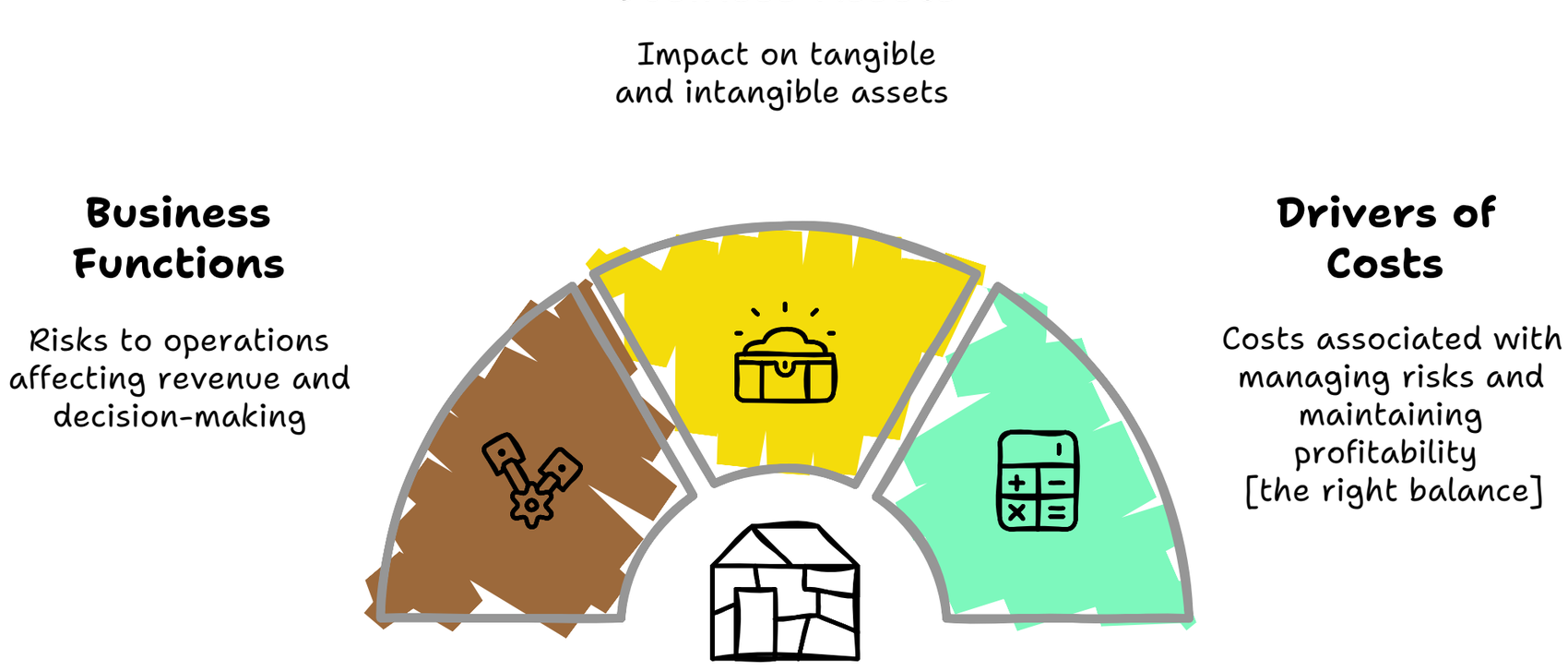
1. **Business Functions**: The activities a business performs to provide services [Risks to business operations] , such as website failure or data loss, can affect revenue or decision-making.
2. **Business Assets**: Anything that has measurable value. Risks that impact both tangible assets (like computers, 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



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.

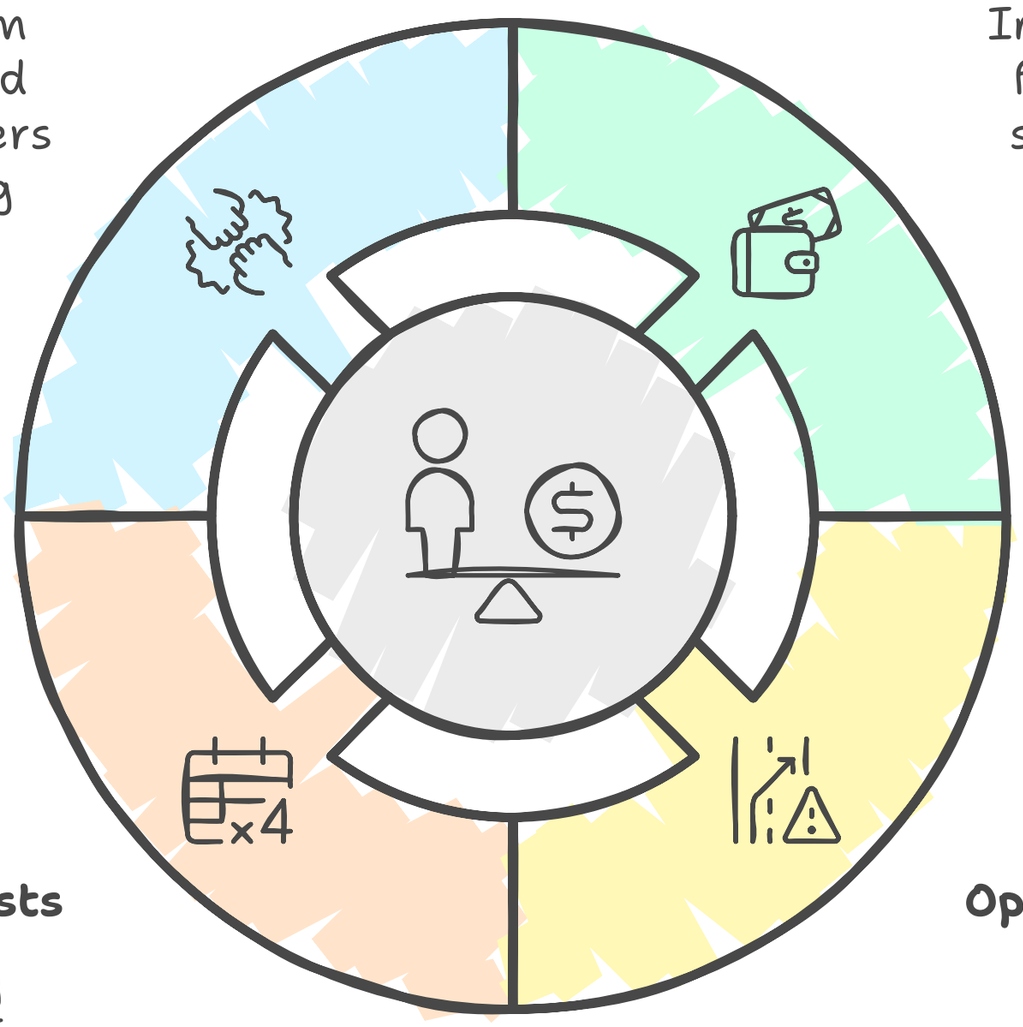
4- Client/stakeholder confidence—The value of client and stakeholder confidence is also important. If risks aren't addressed, clients or stakeholders may lose confidence when a threat exploits a vulnerability, resulting in a significant loss to the company.

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 }] .
   some malwares can releases worm components that can spread across the network.

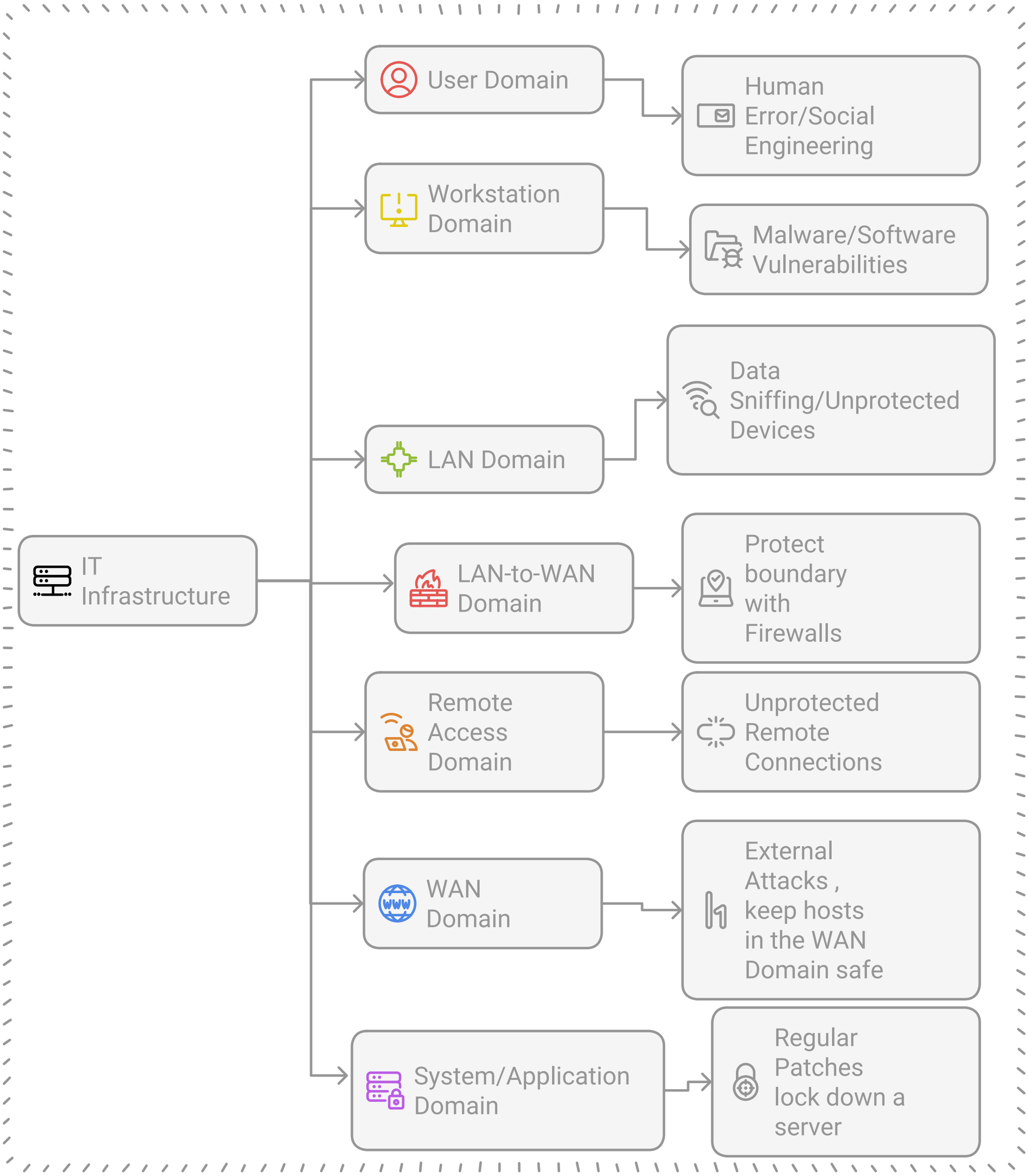
3. **LAN Domain**: Risks within the internal network [the area that is inside the firewall], if each individual device on the network not protected all devices at risk ,the internal LAN is considered as a trusted zone.
   sniffing attack occur when an attacker uses a protocol analyzer to capture data 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.

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 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.

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



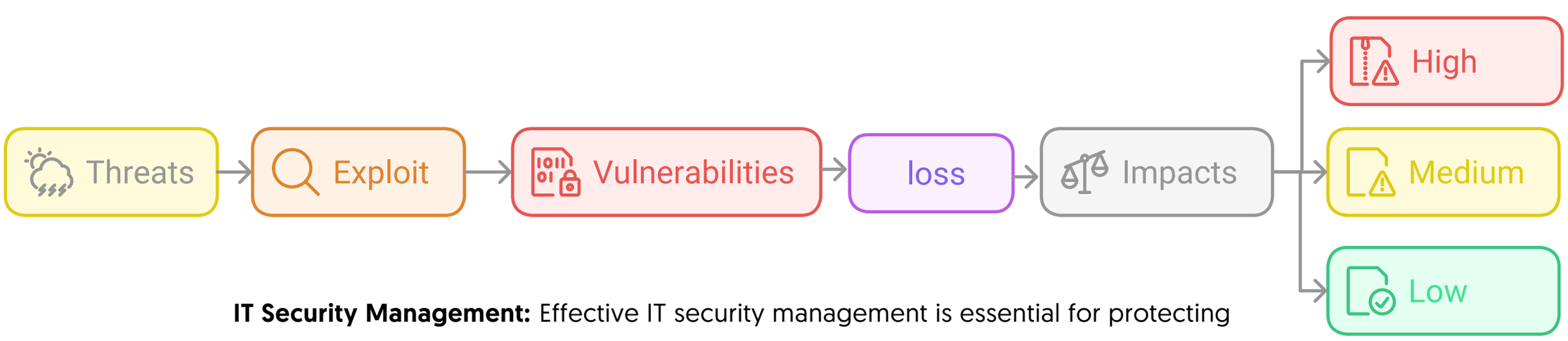
Threats, Vulnerabilities, and Impacts:

- **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.