300 LEVEL CYBERSECURITY

DEPARTMENT OF COMPUTER SCIENCE,
BINGHAM UNIVERSITY, KARU

CYB 309 – SYSTEMS SECURITY
LECTURE I – SECURITY PRINCIPLES

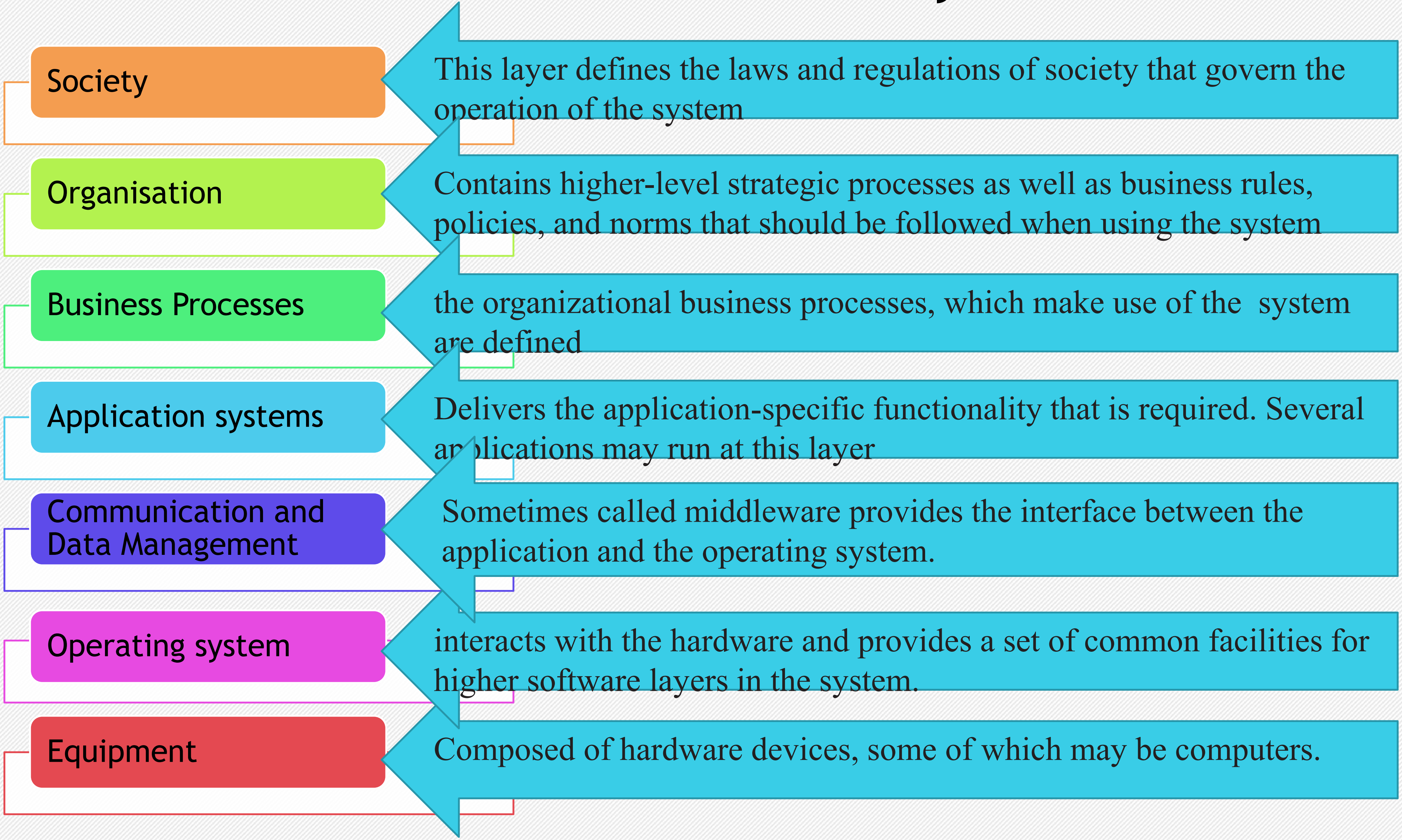
Course outline

- ❖ Introduction
- ❖ Security principles
- ❖ Account Security
- ❖ File system security
- ❖ Risk Assessment
- ❖ Risk analysis
- ❖ Encryption
- ❖ Planning, implementation and auditing of system security package
- ❖ Secure design and secure coding principles, practices and methods including least privilege
- ❖ Threat modelling and static analysis
- ❖ Common vulnerabilities: buffer overruns, integer overflows, injection attacks, cross-site scripting and weak error handling

Introduction - system

- A system is a combination several components (subsystems) working together for the achievement of a common goal.
- The result produced by the combined inputs of the subsystems is more than the sum of the results produced by the subsystems working in isolation. E.g a software system is a mere abstraction of human ideas without a hardware system, relatively, a hardware system a bunch of useless electronics without a software to drive it.
- The properties and usefulness of a system becomes apparent only when the subsystems are integrated and operate together.
- systems that we seek to secure are not isolated systems but rather essential components of more extensive systems that have hardware, software, human, social, or organizational elements.
- This kind of systems is broadly referred to as a sociotechnical system.

Introduction – The sociotechnical system stack



Society

This layer defines the laws and regulations of society that govern the operation of the system

Organisation

Contains higher-level strategic processes as well as business rules, policies, and norms that should be followed when using the system

Business Processes

the organizational business processes, which make use of the system are defined

Application systems

Delivers the application-specific functionality that is required. Several applications may run at this layer

Communication and Data Management

Sometimes called middleware provides the interface between the application and the operating system.

Operating system

interacts with the hardware and provides a set of common facilities for higher software layers in the system.

Equipment

Composed of hardware devices, some of which may be computers.

Introduction - Definition of concepts

Asset: anything of value that could be compromised, stolen or harmed, including information, physical resources or reputation

Threat: An event or action that could potentially cause damage to an asset or interruption of services

Vulnerability: The weakness, flaw, bug or error in a system that a threat could exploit to cause harm to the system. Vulnerabilities could be known or unknown. buffer overflow or buffer overrun vulnerability

Attack: The intentional act of attempting to bypass one or more security services or controls of an information system

Introduction - Definition of concepts – cont’d

Attacker: An attacker, then, is the link between a vulnerability and an exploit. The attacker has two characteristics: skill and will. Attackers either are skilled in the art of attacking systems or have access to tools that do the work for them. They have the will to perform

Exploit: a technique that takes advantage of a vulnerability to perform an attack. May also refer to a packaged form of the technique such as an application or a script that automates the technique so even an unskilled attacker can use the exploit to perform an attack.

Control: A countermeasure that you put in place to avoid, mitigate or counteract security risks due to threats or attack

Information Security Principles

- Information Security principles are general theories about security, technology and human nature in the field of information security. Some of these principles and associated concepts are borrowed from other fields such as military and physical security.

- Since no two systems or situations are identical, and there is no specific procedure on how to solve every security problem. Therefore, security specialist must rely on principle-based analysis and decision making.

- The conceptual and principled view of information security, supports security specialists to analyse every security need in the right frame of reference or context so they can balance the needs of permitting access against the risk of allowing such access.

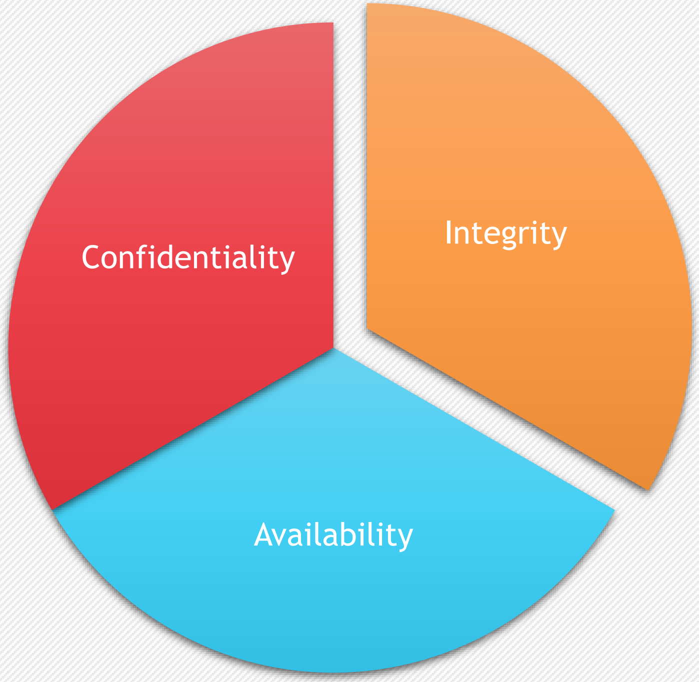
Principle One: There is no such thing as Absolute Security

- Given enough time, tools, skills, and motivation, a malicious party can break through any security measure.
- Security measures simply buy time to delay the malicious parties from achieving their purpose.
- Buying time is a powerful tool as resisting attacks long enough provides the opportunity to catch the attacker in the act and to quickly recover from the incident.

Principle Two: The Three Security Goals are Confidentiality, Integrity and Availability (CIA)

The CIA triad is central to all studies in information/cyber security, thus, all security measures attempts to address at least one of these goals.

Confidentiality also referred to as the principle of least privilege, meaning that users should be given only enough privilege to perform their duties, and no more.



Integrity: The goal of Integrity is to keep data and programs pure and trustworthy by protecting system data and programs from authorised intentional or accidental changes. It supports the following:

- Prevent unauthorised users from making modifications to data or programs.
- Prevent authorized users from making improper or unauthorized modifications.
- Maintain internal and external consistency of data and programs

Availability ensures data and resources are available for authorised use, especially during emergencies or disasters. Information security professionals usually address three common challenges to availability:

- Denial of service (DoS) due to intentional attacks or because of undiscovered flaws in implementation could crash the program if a certain unexpected input is encountered)
- Loss of information system capabilities because of natural disasters (fires, floods, storms, or earthquakes) or human actions (bombs or strikes)
- Equipment failures during normal use

Principle Two: The Three Security Goals are Confidentiality, Integrity and Availability (CIA) Cont'd

Confidentiality models are intended to ensure that no unauthorized access to information is permitted and that accidental disclosure of sensitive information is not possible. They are: access control, authentication, authorisation, encryption, secured data destruction, etc.

Integrity Models: checks is balancing a batch of transactions to make sure that all the information is present and accurately accounted for, Version control, Error correction codes are examples of integrity models.

Availability Models: Some activities that preserve confidentiality, integrity, and/or availability are granting access only to authorized personnel, applying encryption to information that will be sent over the Internet or stored on digital media, periodically testing computer system security to uncover new vulnerabilities, building software defensively, and developing a disaster recovery plan to ensure that the business can continue to exist in the event of a disaster or loss of access by personnel.

Principle Three: Defence in Depth as Strategy

This refers to security implementation in overlapping layers that provide the three elements needed to secure assets: prevention, detection, and response. Defence in depth also seeks to offset the weaknesses of one security layer by the strengths of the other layers.

Defence in depth requires layering security devices/tools in a series that protects, detects, and responds to attacks on systems. For example:

Prevention: Network designed with security in mind includes routers, firewalls, and intrusion detection systems (IDS) to protect the network from would-be intruders.

Detection: Employs traffic analysers and real-time human monitors who watch for anomalies as the network is being used to detect any breach in the layers of protection

Response: Relies on automated mechanisms to turn off access or remove the system from the network in response to the detection of an intruder.

Finally, the security of each of these mechanisms must be thoroughly tested before deployment to ensure that the integrated system is suitable for normal operations.

Principle Four: When Left on their own People are the Weakest Link on the Security Chain

The primary reason identity theft, viruses, worms, and stolen passwords are so common is that people are easily duped into giving up the secret technologies use to secure systems. The weakness in people manifest in their:

- Susceptibility to social engineering
- Poor password management
- Inability to follow policies
- Poor configuration management, etc

Principle Five: Computer Security Depends on two Types of Requirements: Functional and Assurance

- ❖Functional requirements describe what a system *should* do.
- ❖Assurance requirements describe how functional requirements should be implemented and tested.

For example:

- ❖The functional requirement for a network security is to put in place preventative, detection and response mechanisms;
- ❖The security assurance requirements is describes how these mechanisms are implemented and tested regularly for workability.

Both sets of requirements are needed to answer the following questions:

✓Does the system do the right things (behave as promised)?

✓Does the system do the right things in the right way?

Principle Six: Security through Obscurity is not an Answer

Security through obscurity means that hiding the details of the security mechanisms is sufficient to secure the system. An example of security through obscurity might involve closely guarding the written specifications for security functions and preventing all but the most trusted people from seeing it.

- ❖Obscuring security leads to a false sense of security, which is often more dangerous than not addressing security at all.
- ❖If the security of a system is maintained by keeping the implementation of the system a secret, the entire system collapses when the first person discovers how the security mechanism works.

- ❖The better bet is to make sure no one mechanism is responsible for the security of the entire system. Again, this is defence in depth in everything related to protecting data and resources.

Principle Seven: Security = Risk Management

❖Securing systems involves a careful balance between the level of risk and the expected reward of expending a given amount of resources.

❖Thus, it is critical to understand that spending more on securing an asset than the intrinsic value of the asset is a waste of resources.

❖Risk assessment and risk analysis are concerned with placing an economic value on assets to best determine appropriate countermeasures that protect them from losses.

When risks are well understood, three outcomes are possible:

✓The risks are mitigated (countered).

✓Insurance is acquired against the losses that would occur if a system were compromised (Risk Transfer).

✓The risks are accepted and the consequences are managed (Risk Acceptance).

determining the degree of a risk involves looking at two factors:

- What is the consequence/impact of a loss?
- What is the likelihood that this loss will occur?

Principle Eight: The three types of Controls are: Preventative, Detective and Responsive

security mechanism serve a purpose by:

- Preventing a compromise,
- Detecting that a compromise or compromise attempt is underway,
- Responding to a compromise while it’s happening or after it has been discovered.

✓This is referred as defence in depth

✓The purpose of these control is to achieve the goals of the CIA

✓These controls are applied through the people, process technology (PPT) framework

Principle Nine: Complexity is the Enemy of Security

- The more complex a system gets, the harder it is to secure.
- With too many “moving parts” or interfaces between programs and other systems, the system or interfaces become difficult to secure while still permitting them to operate as intended.
- Consequently, it is advised that systems are developed with less complexity to ease managing their security.

Principle Ten: Fear, Uncertainty and Doubts do not work in selling Security

At one time, "scaring" management into spending resources on security to avoid the unthinkable was effective. However;

- The tactics of fear, uncertainty, and doubt (FUD) no longer works: Information security and IT management is too mature continue in that direction.
- Now IS managers must justify all investments in security using techniques of the trade. Although this makes the job of information security practitioners more difficult, it also makes them more valuable because of management's need to understand what is being protected and why.
- When spending resources can be justified with good, solid business rationale, security requests are rarely denied.

Principle Eleven: People, Process and Technology are needed to adequately Secure Systems

- The vulnerabilities in People, Process and Technologies will have to be addressed to secure systems
- Similarly, People, process and technology are tools for securing systems.

For example:

Processes are documented on how to secure systems. Example:

- The process of configuring a server operating system for secure operations is documented
- Procedures that security administrators use and can be verified as done correctly.
- Process controls to make sure that a single person cannot gain complete control over a system

People are needed design the policies/procedures that will govern the security of the assets

Technology provides the mechanisms to enforce what the people document in the processes. Example, password length and combination.

Principle Twelve: Open Disclosure of Vulnerability is Good for Security

The debate within the security community and software developing centres concerns whether to let users know about a problem before a fix or patch can be developed and distributed.

- Principle 6 says that security through obscurity is not an answer, that is keeping a given vulnerability secret from users and from the software developer can only lead to a false sense of security.
- Users have a right to know about defects in the products they purchase.
- The need to know trumps the need to keep secrets, to give users the right perspective to the state of security of the products they use.

Account security

A **user account** is an identity created for a person (user) in a computer or computing system to enable them have access to the system’s resources.

Interactive Account - a Standard User Account
The normal user account for a person is also called an interactive account or a standard user account. Such users can usually be used to log in using a password and can be used for running programs on the computer.

Privileged Account Management (PAM)
Privileged accounts, and particularly root and administrator accounts, grant high level privileges on computers. They can be used to:

- Modify important data;
- Change system configuration;
- Install and remove software;
- Upgrade the operating system.

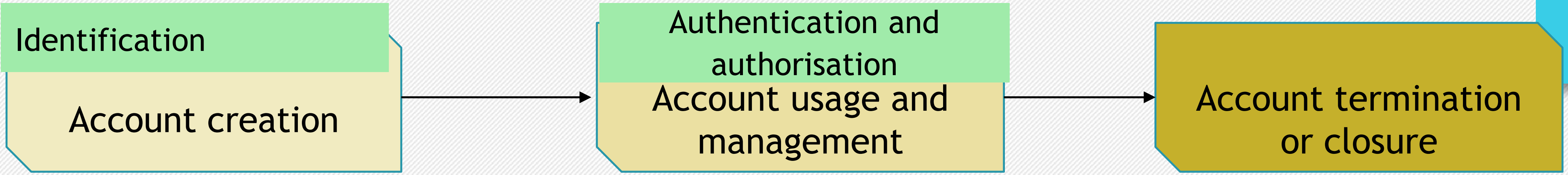
Managing and monitoring privileged accounts is thus very important for preventing systems compromise as they can be used by malicious parties to:

- Steal information,
- Hide one's actions

etc

Account security through Identity and Access Management (IAM)

IAM systems supports organisations to maintain optimal data security by ensuring the appropriate users get access to only the information essential to their role.



Identification

Account creation

Authentication and authorisation

Account usage and management

Account termination or closure

Account creation **policy** that defines account creation rules such as:

- Identification rules
- Who requests account creation
- Structure of user name
- Length and make-up password (number and types of characters)
- Enforcement of default password change

Collection of login Data

- Multifactor authentication (MFA)
- Biometrics (finger prints, iris, facial recognition, DNA)

Managing User Credentials

- Mechanisms to enforce passwords change at defined intervals

Assigning access permissions

- Determine sensitivity of information
- Determine permission to information based on sensitivity: example:

✓ Lower privilege users to lower sensitive data

✓ Higher privilege users to higher sensitive data

- Account termination policy that defines account termination rules such as:
- Timing for user account termination
- Mechanisms for user accounts termination

Authentication is the process of assessing the identity of a subject so that an IAM system can ensure the right person is accessing secure information.
Authorization refers to the levels of permission allowed for authenticated users. So, some authenticated users might not be authorized to access certain data.

File system security

File security entails safeguarding organisation’s critical information from threat actors by:

- ❖Implementing stringent access control measures and flawless permission hygiene;
- ❖Enabling and monitoring security access controls,
- ❖Decluttering data storage (remove files saved multiple times, etc);
- ❖Regularly optimize file storage by purging old, stale, and other junk files to focus on business-critical files;
- ❖Tackle data security threats and storage inefficiencies with periodic reviews and enhancements to your file security strategy;

File system security – Importance

- **To protect sensitive data**

Personally identifiable information (PII), electronic personal health information (ePHI), confidential contracts, intellectual property data, etc must be stored safely. Careless transmission or use of such files could lead to data privacy violations, resulting in legal or regulatory penalties (fine, litigations and claims)

- **To secure file sharing**

Files transferred through unsecured channels can be misused by insiders or hackers for malicious activities. Comprehensive data leak prevention software can help prevent unauthorized movement of business-critical data out of the organization.

- **To avoid data breaches**

The impact of such a breach can be fatal to any organization. It is not just the fines and legal consequences, but also the loss of trust and reputation that can destroy a business.

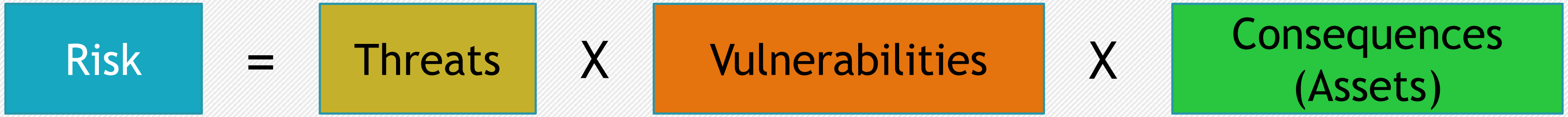
File system security – Best Practices

- **Eliminate permission hygiene issues -** The principle of least privileges (POLP) ensures that only the bare minimum privileges required to complete a task is granted. It is advisable to define access control lists (ACL) for files and folders based on user roles and requirements.
- **Secure file sharing channels -** All file transfers should be authorized and secure. Audit all the possible ways files can be transferred, and block private devices like personal USB drives.
- **Implement file server auditing -** Be wary of multiple failed accesses, bulk file renames, or modifications. Mass, unofficial file modifications such as delete events may indicate a ransomware attack.
- **Enforce authentication and authorization protocols -** Enforce multi-factor authentication (MFA) for all users in your organizations. MFA makes it difficult for hackers to penetrate the network. Authorize only valid and official data access requests.
- **Conduct file storage analysis -** Analyze and manage your file repositories periodically. Know where your critical files are stored in the organization. Continuous review of stale files and unused files helps eliminate permission misuse incidents. Revoke permissions on files owned by former employees

Risk Management

Risk

- is a measure of an asset’s exposure to the chances of damage or loss.
- It is the likelihood of a hazard or dangerous threat to occur.
- Is associated with loss of system power, network, etc
- Its also affects people and processes/practices
- Risk is composed of three factors; threats, vulnerabilities and consequences (assets)



Risk = Threats X Vulnerabilities X Consequences (Assets)

- Ransomware
- DDOS
- Natural Disaster

- people
- Technology
- Processes

Services/assets

Business Impact

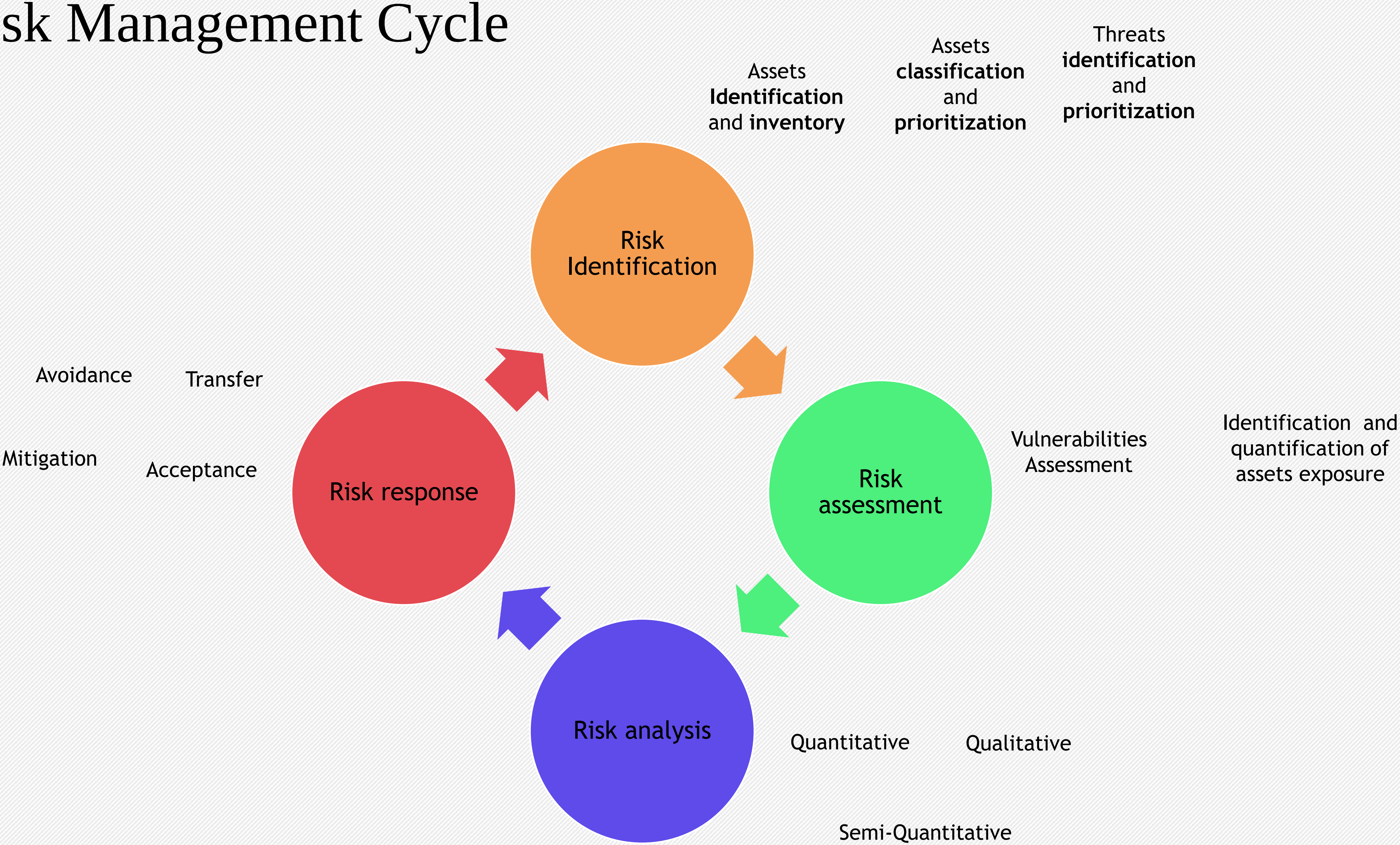
- Angry customers
- Unplanned spending
- Litigation
- Reputational damage
- Loss of competitive advantage
- Loss of stakeholders confidence

Impact of Risk on Organisation

Risk can impact an organisation in the following ways:

#	Risk Type	Impact
1	legal	Organisations must operate in compliance with laws and regulations within its environment. Failure will lead to service of legal notice, penalties and litigations that eventually impact profits
2	Financial	Certainly threats are targeted at the financial expectations of organisations which ultimately affects their survivability. E.g lost hours due to failed systems, cost of replacement, increased insurance cost, etc
3	Physical Assets	Human threats and environmental factors may put your physical assets at risk of damage or theft; leading to losses that will negatively impact business.
4	Intellectual property	Intellectual property (e.g copyrights, trademarks, etc) may be altered or destroyed in a manner that makes it extremely difficult to recover. Other threats like sophisticated data exfiltration techniques will make it difficult for you to spot a breach of your intellectual property.
5	Infrastructure	ICT infrastructure (hardware, software, data management, services, network) are faced with threats of different nature (nature, human and technology). Infrastructure risk impact the organisation at foundational level.
6	Reputation	The public perception of an organisation has potentials to ruin the organisation (if its negative). Attacks that lead theft of personal data (e.g PII) can negatively impact an organisation's public perception.
7	Operations	Daily running of the organisation may be impeded by risk that affects the smooth running of its operations leading to poor services, poor productivity, etc.
8	Health and Safety	

Risk Management Cycle



Risk Identification

Assets **Identification** and **inventory**

Assets **classification** and **prioritization**

Threats **identification** and **prioritization**

Risk assessment

Vulnerabilities Assessment

Identification and quantification of assets exposure

Risk analysis

Quantitative

Qualitative

Semi-Quantitative

Risk response

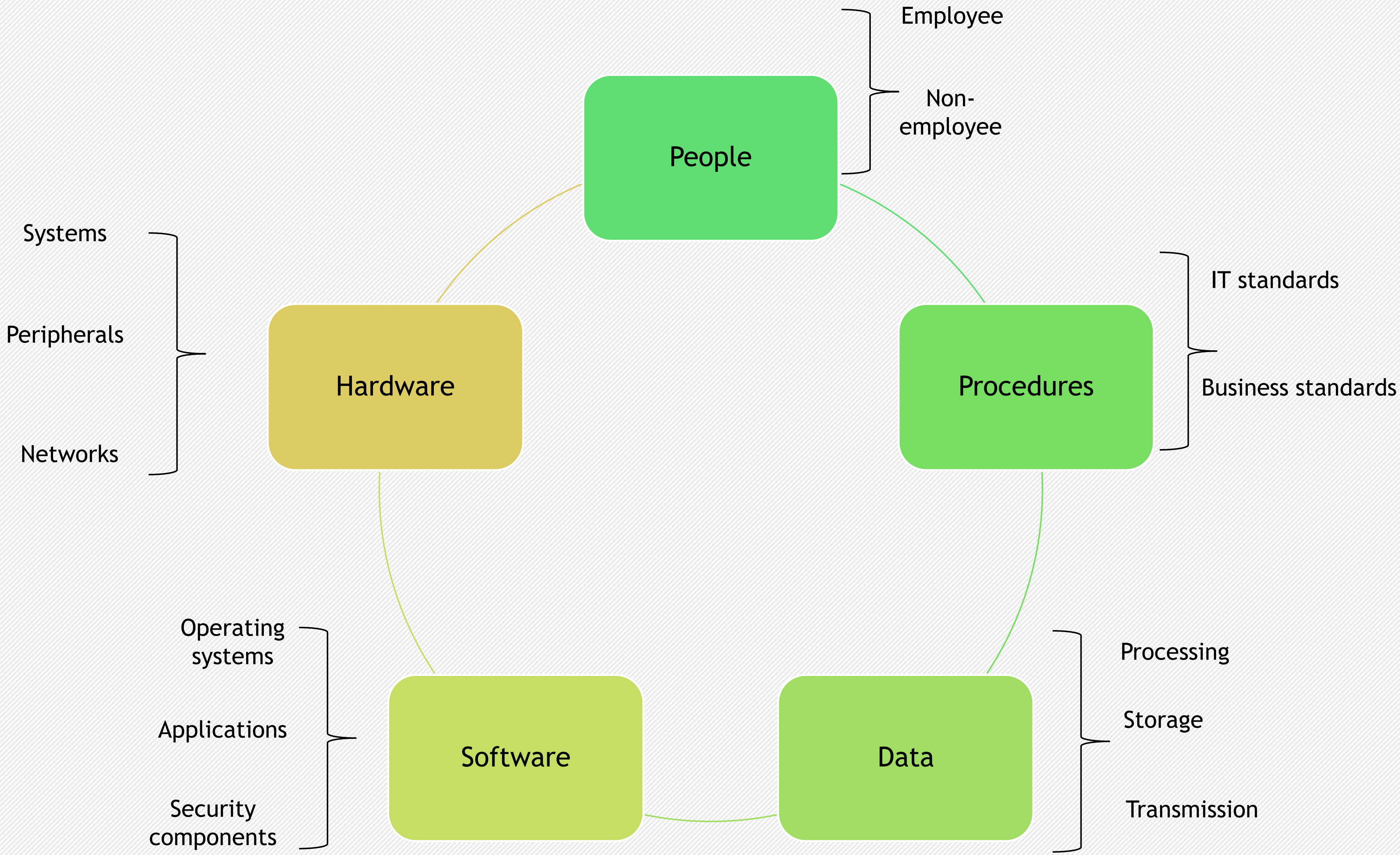
Avoidance

Transfer

Mitigation

Acceptance

Asset Identification



Information Asset classification

Based on value of assets

- Cost of creating the information asset
- Retained from past maintenance of information asset
- Cost of replacing information
- Value from providing the information
- Value to owners
- Intellectual property value
- Value to adversaries

Based on impact

- Impact on revenue
- Impact on profitability
- Impact on public image or reputation

Based Data/information Classification Levels

- Public
- Internal only
- Confidential
- Restricted

Threats Identification and Prioritization

Threats are assessed on the basis of potential damage to assets as follows:

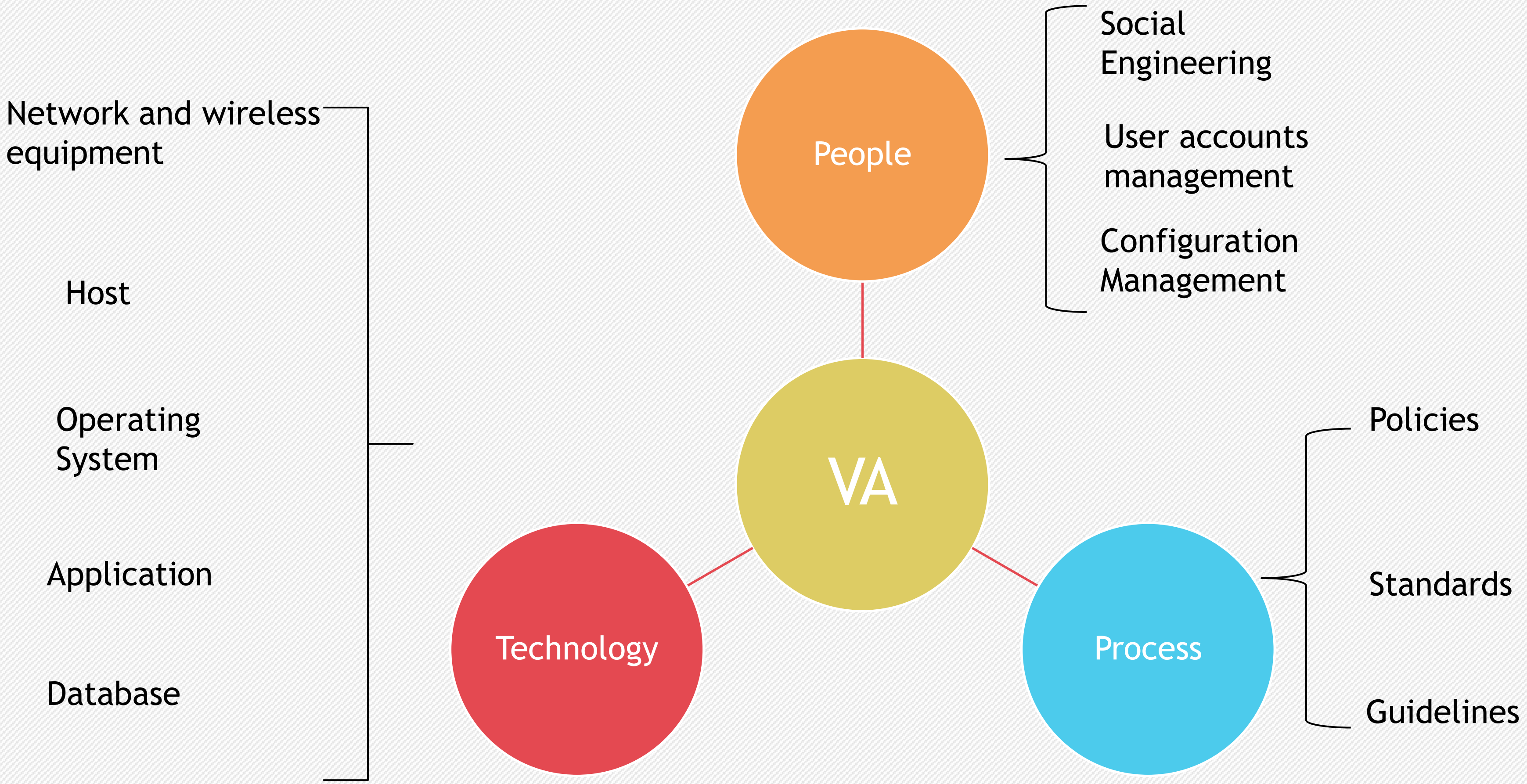
- ❖Threats that present danger to an organization's assets
- ❖Threats that represent the most danger – with highest probability of attack?
- ❖The cost of recover if the threat successfully compromises or damage an asset?
- ❖The threat that requires the greatest expenditure to prevent from exploiting organisation's assets

Threats Identification and Classification – cont’d

SN	Threats	Examples
1	Intellectual property compromise	Piracy, copyright infringement
2	Espionage or trespass	Unauthorized access
3	Nature	Fire, flood, earthquake, lightning
4	Human error or failure	Accidents, mistakes, etc
5	Poor controls or processes	Training, privacy, ineffective policy
6	Deviation of quality of service	Power and WAN quality of service
7	Sabotage or vandalism	Destruction of systems or information
8	Software attacks	Viruses, worms, macros, DOS
9	Technical failure - hardware	Equipment failures
10	Technical failure - software	Bugs, code problems, loopholes
11	Technological obsolescence	Antiquated or outdated technology
12	Theft	Illegal confiscation of property

Risk assessment – Vulnerabilities Assessment (VA)

VA is the process of defining, identifying, classifying and prioritizing vulnerabilities in People Process (policies and procedures) and technology (computer systems, applications and network infrastructures).VAs provide an organization with the necessary knowledge, awareness and risk backgrounds to understand and react to threats within its environment.



VA

People

- Social Engineering
- User accounts management
- Configuration Management

Process

- Policies
- Standards
- Guidelines

Technology

- Network and wireless equipment
- Host
- Operating System
- Application
- Database

Risk assessment – Identification and Quantification of Exposure

Risk exposure is the property that indicates how susceptible an organisation is to loss.

Likelihood refers to the Probability that a specific asset within the organisation will be successfully attacked. It is assigned number between 0.1 – 1
There are predefined values for some factors, example:

- Likelihood of fire
- Likelihood of receiving infected email
- Number of network attacks
- **Impact of loss** is the value of the asset which is determined by the following factors:
- Cost of creating the information asset
- Retained from past maintenance of information asset
- Implied by the cost of replacing information
- Value from providing the information
- Value to owners
- Intellectual property value
- Value to adversaries

Risk assessment – Quantification of Exposure

Quantitatively, it is defined as:

Probability (Likelihood) that an event will occur X the Impact of loss if it occurs.

For example, if the estimated likelihood of occurrence of a ransomware attack on the data of an organisation is 0.1 and the expected impact of loss of data due to that attack is NGN1,000,000.00,

The risk exposure will computed thus:

Likelihood = 0.1, Impact = 1,000,000.00

Exposure = Likelihood X Impact

Exposure = 0.1 x 1000000

Exposure = NGN100,000.00

Risk Analysis

Quantitative Risk Analysis- is based completely on numeric values. Data is analysed using historical records, experiences, industry best practices and records, statistical theories, testing and experiments.

Qualitative Risk Analysis – Uses words and descriptions to measure the impact and likelihood of risk. Example: High, moderate, medium or low; likelihood rating can be likely, unlikely or rare.

Semi-Quantitative Risk Analysis-Finds a middle ground between quantitative and qualitative risk analysis, its creates a hybrid risk analysis methodology. It helps to measure risk variables like reputation, employee motivation, etc

Risk Responses

Organisations can respond to risk by avoidance, transfer, mitigation and acceptance.

Avoidance - Eliminate the threat to protect the project from the impact of the risk. An example of this is cancelling the project.

Transfer - Shifts the impact of the threat to as third party, together with ownership of the response. Example: transfer the risk to an insurance

Mitigation - Act to reduce the probability of occurrence or the impact of the risk.

Acceptance - Acknowledge the risk, but do not take any action unless the risk occurs. For instance, document the risk and putting aside funds in case the risk occurs.