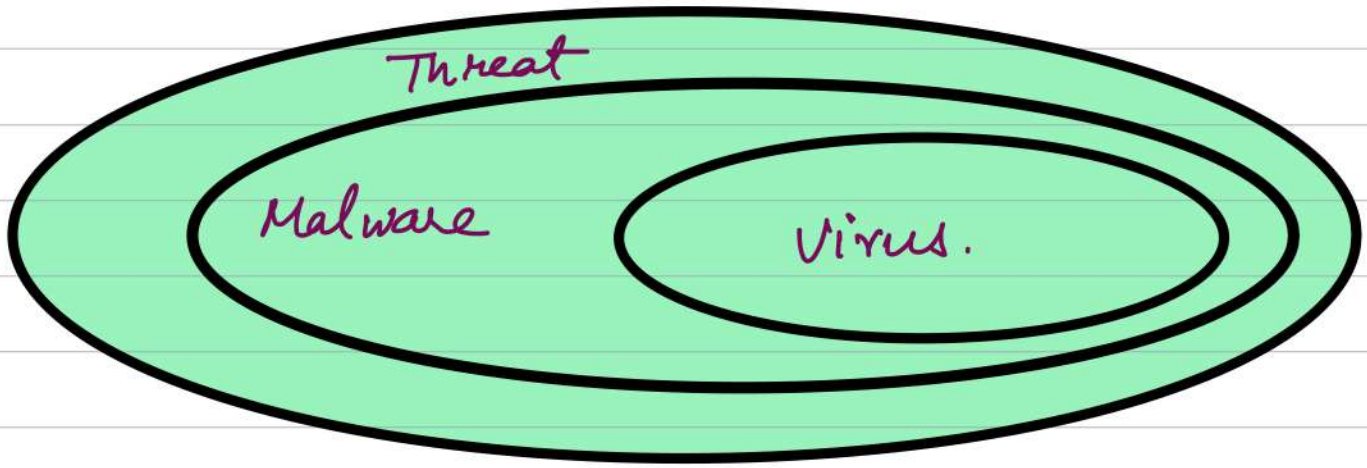
Threat, Malware, and Virus



It share two defining traits :—

1. They are sneaky.
2. They are actively working against your best interest!

Terms :—

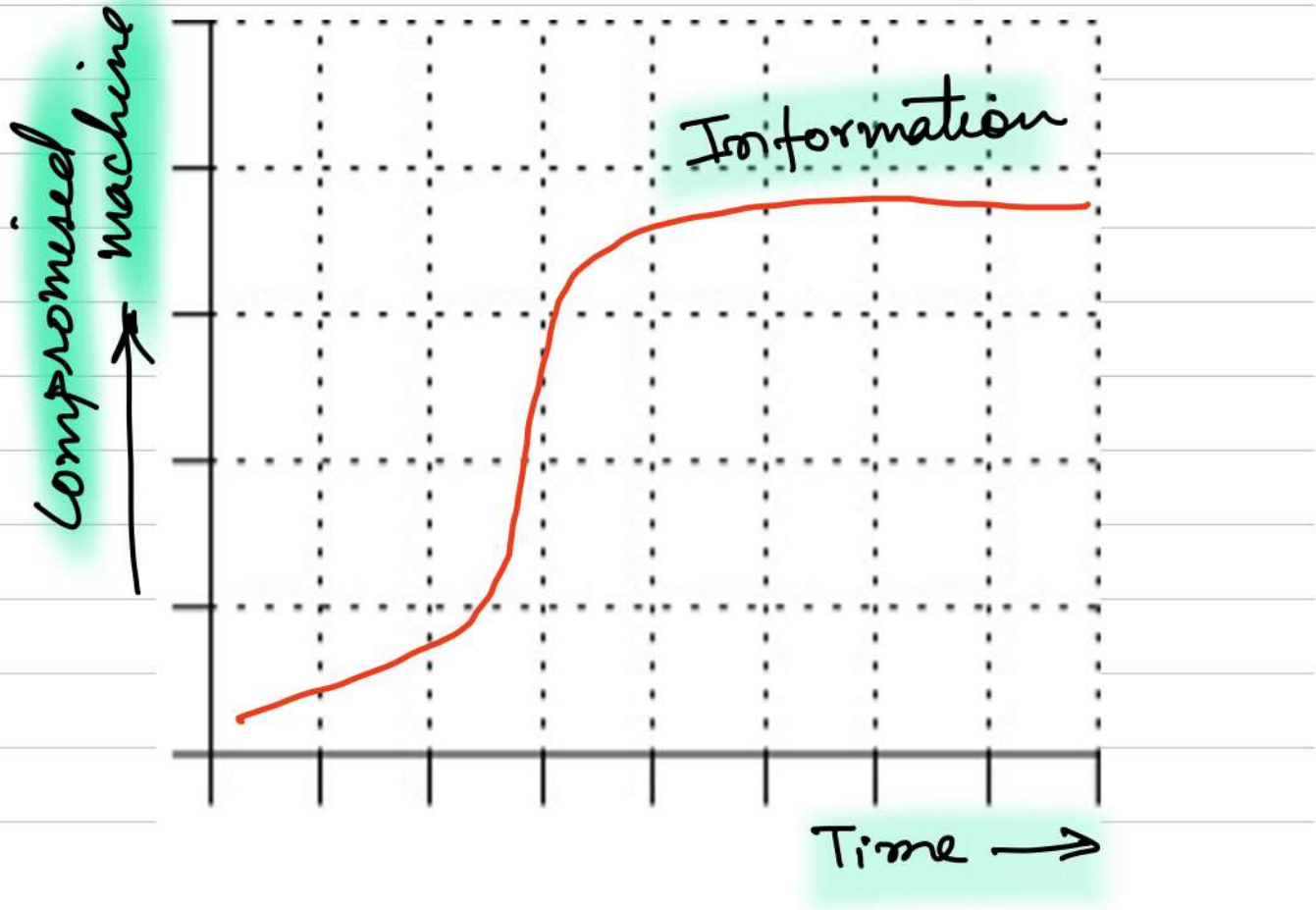
1. SPAM! — Email Traffic.
2. Bugs :- S/W error, data corruptions.
3. Denials of Service (DOS) :— Starve legitimate usage resources.

(4) Malicious S/W :— Malware and

Malware S/W specific threats, Virus, worms, Trojan Horse and Spyware.

Cost of Malware

- Hidden Cost
  - Leak of private information
- Real cost
  - which you can measure.



Virus :— There are four phases or life cycle.

1. Dormant Phase.
2. Propogation Phase.
3. Triggering Phase.
4. Execution Phase.

Spreads :—

Email, Downloads, Messaging Services, Old S/W, Malvertising, File sharing, Infected H/W, Fake Antiviruses.

Computer Virus :—

Bootsector, Overwrite, Resident, File-transfer, Macro, Web-scripting, Polymorphic, Multi-partite.

Symptoms :-

↳ Slow, corrupted, pop-ups, program failure, spinning H/w, Malfuctioning apps, files, and other programs.

Prevention :-

↳ Antivirus s/w, updated and genuine s/w, Enable Firewalls, Don't open suspicious Emails, Adjust Privacy settings (devices and browser).

Malware Functions :—

(1) Self-Replicating Malware :—

↳ Create new copies

↳ Instance of itself.

(2) Population Growth :—

↳ Overall change in No. of Malware instances.

(3) Parasitic Malware :—

↳ Its required some other executable code to exist.

Various Malwares :—

(1) Logic Bomb :—

↳ It has a legitimate code.

ex:- { If date is Friday the 13th:
Crash_computer();

legitimate code.

- Self-Replicating :- No
- Population Growth :- Zero.
- Paracitic :- Possible.

Work:-

① Payload:- Action to perform.

② Trigger:- A boolean condition that is evaluated and control when payload executed.

Syntax:- Code:-

```
if date is Friday the 13th;
    Crash_computer();
legitimate code();
```

(2) Trojan Horse :-

- Self-Replicating :- No
- Population Growth :- Zero.
- Parasitic :- Yes

↳ The program/s/w that create the backdoor when it infect the system.

↳ used for :- Payload execution, Password-grabbing.

(3) Backdoor :- It is an mechanism which bypass a normal security check.

Ex :- RAT :- Remote Administration Tool and Remote Access Trojan

Syntax:-

```
username = read_username();
password = read_Password();

if (username == "12345")
    return Allow_login;

if (username and Password) == valid
    return Allow_login;
else:
    return Deny_login.
```

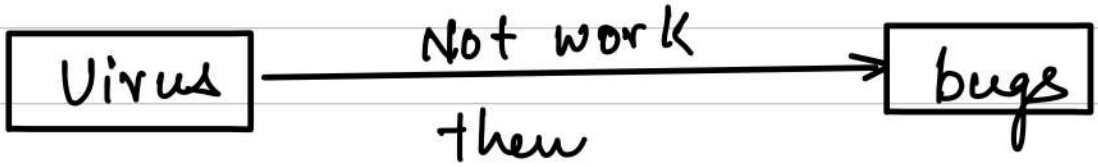
(4) Virus

↳ it is malware.
↳ it replicate itself into other executables.
↳ it infect the codes.
↳ The infected code can infect new codes.
↳ self-Replicating is the Key characteristices.
↳ Not propagate through N/w.

- self-Replicating = Yes
- Population Growth = Positive
- Parasitic = Yes

Propogations :-

↳ Human-transported media
↳ CD-ROM, USB drive.



Life Cycle of Virus

1. Dormant Phase.
2. Propogation Phase.
3. Triggering phase.
4. Execution Phase.

Spreads:- Email, Downloads, Messaging, Services, old s/w, File sharing, Infected H/W, Fake Anti viruses.

(5) Worm :-

↳ It shares several characteristics with a virus.

↳ They are of two types :-

(1) standalone :- Does'nt rely on other codes.

(2) worm spread from machine to machine accross network.

- self - Replicating = Yes
- Population Growth = Positive
- Parasitic = No

(6) Rabbit

- self - Replicating = Yes
- Population Growth = Zero
- Parasitic = No

→ Rabbit is the term used to describe malware that multiplies rapidly.

→ Rabbit may also be called Bacteria

There are two types of rabbit:—

① The first is a program which tries to consume all of system resources like (Disk space).

Ex:— "Fork bomb" → It is a program which creates new processes in an infinete loop.

② Second kind of rabbit is special kind of worm.
↳ standalone pgm which replicates itself.
↳ Delete original copy of itself after replication.

Ex:—
```
while true
do
mkdir x
chdir x
done
```

⑦ Spyware

- self-Replicating = No
- Population Growth = Zero
- Parasitic = No

↳ Collects info to the computer and transmits to someone else.

↳ Used for:-
  ↳ Key logging
  ↳ Recording video and Audio.
  ↳ Remote control.
  ↳ Browser History

↳ Spyware Gatheres
  ↳ username and password
  ↳ Email Address.
  ↳ Bank Account (S/w license Keys)

↳ Virus and worms do the same but spyware doesnt self-replicates.

Types of Spyware

↳ Pwd stealers.
↳ Banking Trojan Malware.
↳ Info stealers.
↳ Key loggers.
↳ Browser Hijacking.

(8) Adware

- self-Replicating = No
- Population Growth = Zero
- Parasitic = No

↳ It gather info about users and their habits.

↳ Create pop-up advertisement or redirect users web-browser request to certain website.

(9) Zombies

↳ The computer that name/IP/MAC is compromised can be used by an attacker for variety of tasks.

↳ without the knowledge of original user.

↳ Task perform
  ↳ sending SPAM.
  ↳ Large Scale Dos Attacks.
  ↳ Flooding N/W Traffic.

(10) Scareware

↳ Attacker scare user to think that the computer or smartphone have become infected.

Result:- Victim purchase the application.

Warning:- Computer is infected.
Cannot be removed easily.

(11) Ransomware:-

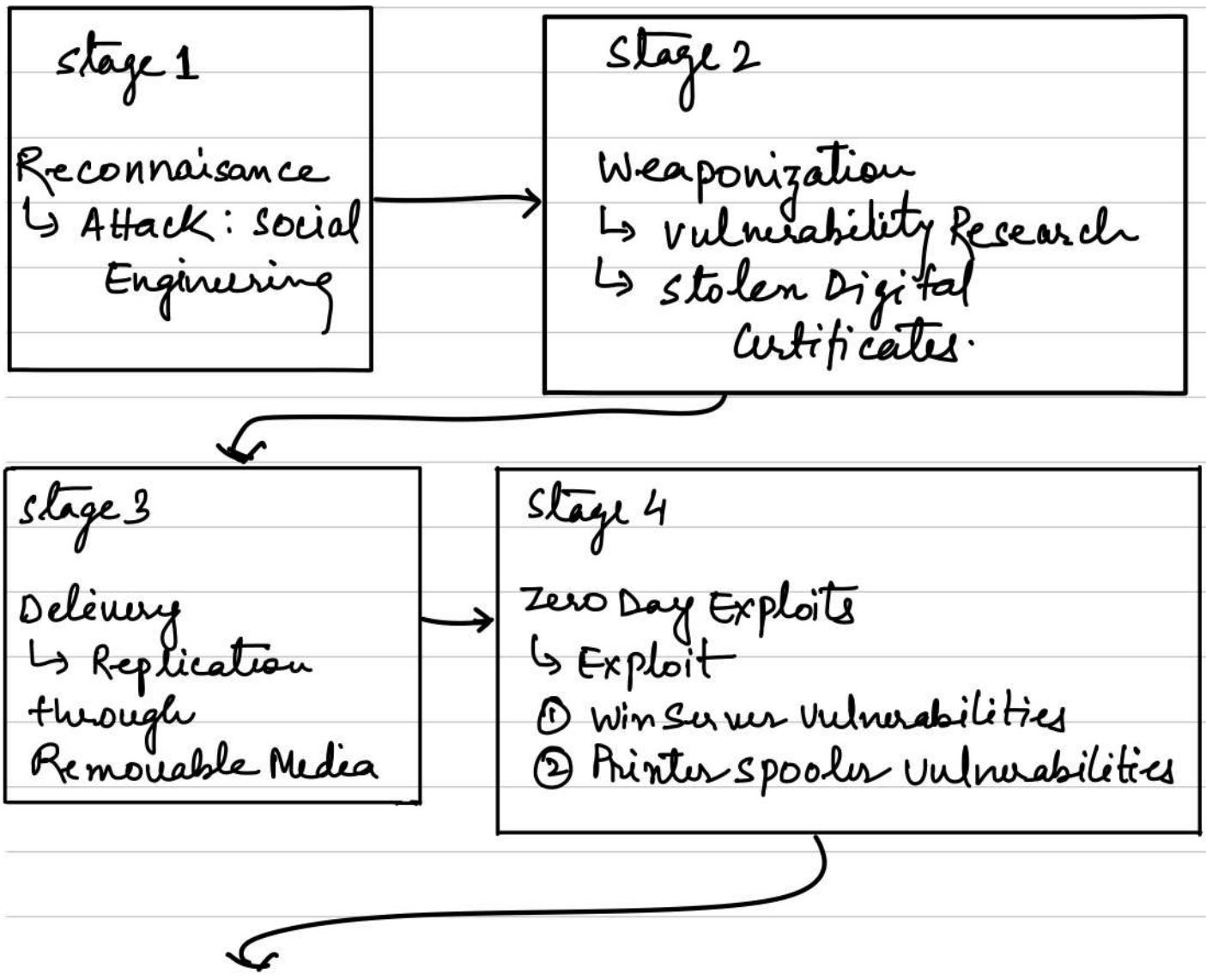
- self-Replicating = No.
- Population Growth = Yes.
- Parasitic = Possible.

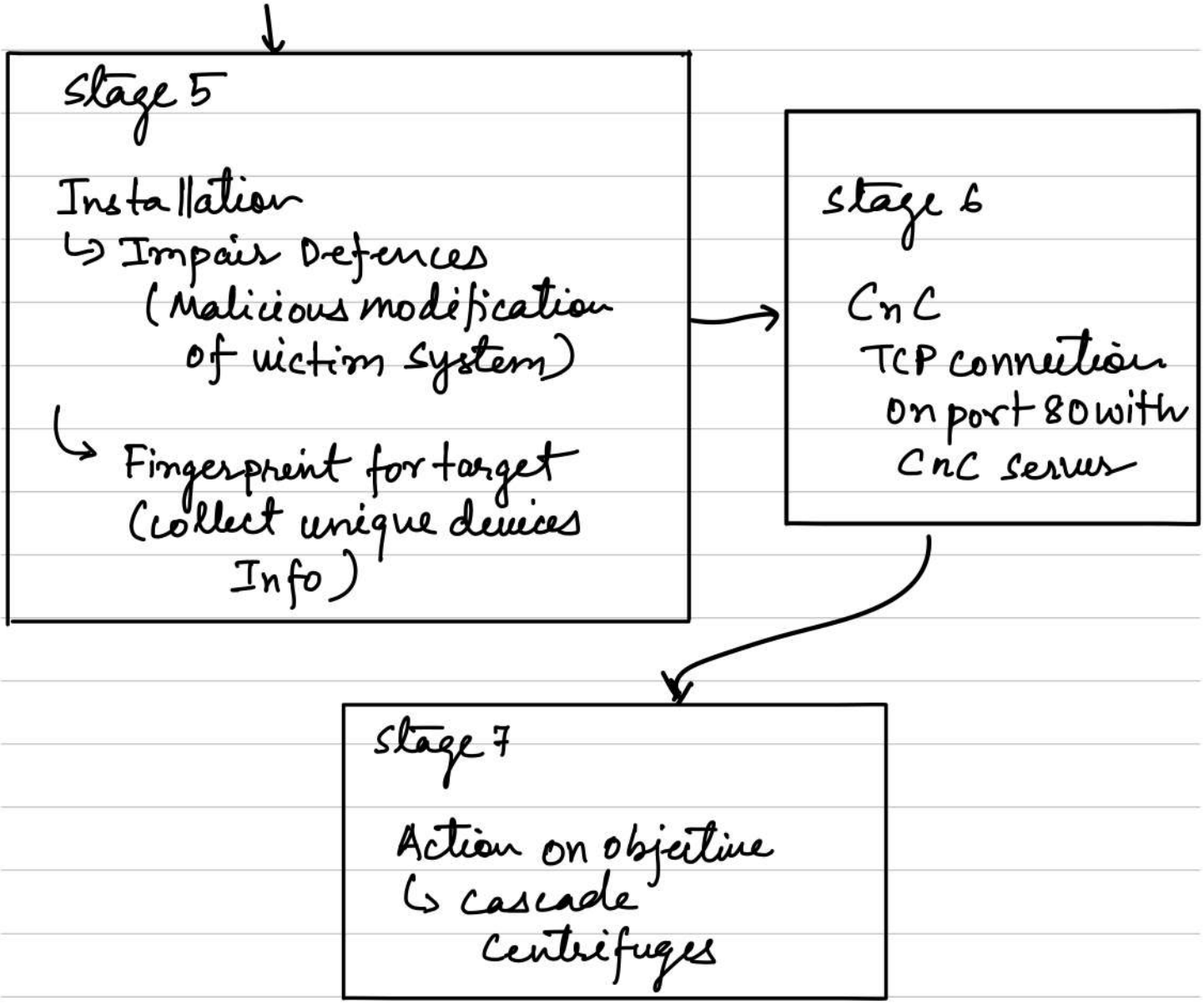
↳ encrypt the files and even entire computer system.

↳ Attack Perform

↳ File corners.
↳ Doxxing
↳ Screen lockers.

STUXNET VIRUS





Imp Question :-

Q How C&C servers are used and what is the malicious use of C&C server at stuxnet virus.

Answer :- Command and control server

↳ Provide communication b/w Botmasters and the infected devices (IOT).

We use C&C for two reasons :-

① The bots are unique and unlikely to change among bots and their variants.

② It act as communication hub, enabling botmasters to issue commands and co-ordinate malicious activities.

- Botmaster setup the C&C server, typically an IRC (Internet Relay chat) server.

The C&C system is classified as :-

① Centralized C&C Model

↳ It is a predominant model which is used by existing botnets

↳ Ex:- Agobot, SDBot, RBOT.

↳ The single high bandwidth host is used for contact point for all the bots.

↳ It run the services like HTTP/IRC/etc.

↳ The infected computer by bots, will join the botnet by C&C server.

↳ The botmasters execute the command on C&C server.

↳ IRC channels may be password-protected to prevent eavesdropping.

Reason for adoption

↳ uses widely available tools like IRC bot scripts.

↳ control thousand of bots which increase the profit.

↳ Ensure coordinated attack execution.

- Destroying the bots can dismantle the entire N/W.

P2P-based C&C Model

↳ It is more resilient to failure than centralized.

↳ It wont rely on single server, which makes botnet harder to discover and destroy.

↳ It support 10-50 users.
  ↳ It is harder to coordinate large-scale Attack.
  ↳ It may grow in future, currently its is robust in nature.

Random C&C Model

↳ Not yet used in Real-world but offer high resilience.

↳ The botmaster scan the bot to execute the commands.

↳ Difficult to detect.
  ↳ Hard to manage large botnets.
    ↳ Not suitable for Synchronized Attacks.

Malicious use of C&C servers

1. Infecting new hosts.
2. Stealing Personal Info.
3. Phishing and Spam Proxy
4. DDoS.

Risk Management :-

↳ N/W Vulnerabilities :-

↳ ① outdated Application :-

Failing to ↳ update, test, patch.

↳ ② Security GAPS :-

↳ Insure direct object.

ISO 27005 : Risk Management workflow for Cyber Security.

① Context Establishment.

↳ scope, objective, and Criteria.

↳ Identify Internal and external factors.

(2) Risk Assessment :-

Risk Analysis

- **Risk Identification :**
  - ↳ list Potential risk that impact objective
- **Risk Estimation :**
  - ↳ Quantify the likelihood and impact.
- **Risk Evaluation :-**
  - ↳ compare risk level against criteria to prioritize.

(3) Risk Treatment :-

strategies ↳ Mitigate, transfer, accept, or avoid risk.

Effective ↳ Regular monitor.

(4) Risk Decision Points :-

↳ Points 1 :- Assessment satisfactory.

↳ Point 2 :- Treatments are Sufficient.

(5) Risk Acceptance :-

↳ Accept the remaining risk after treatment.

↳ Mark the end of the current risk management iterations.

(6) Risk Communication :-

↳ sharing of finding, progress, and action.

(7) Risk Monitoring and Review :-

↳ Observe and detect changes and refine the process.

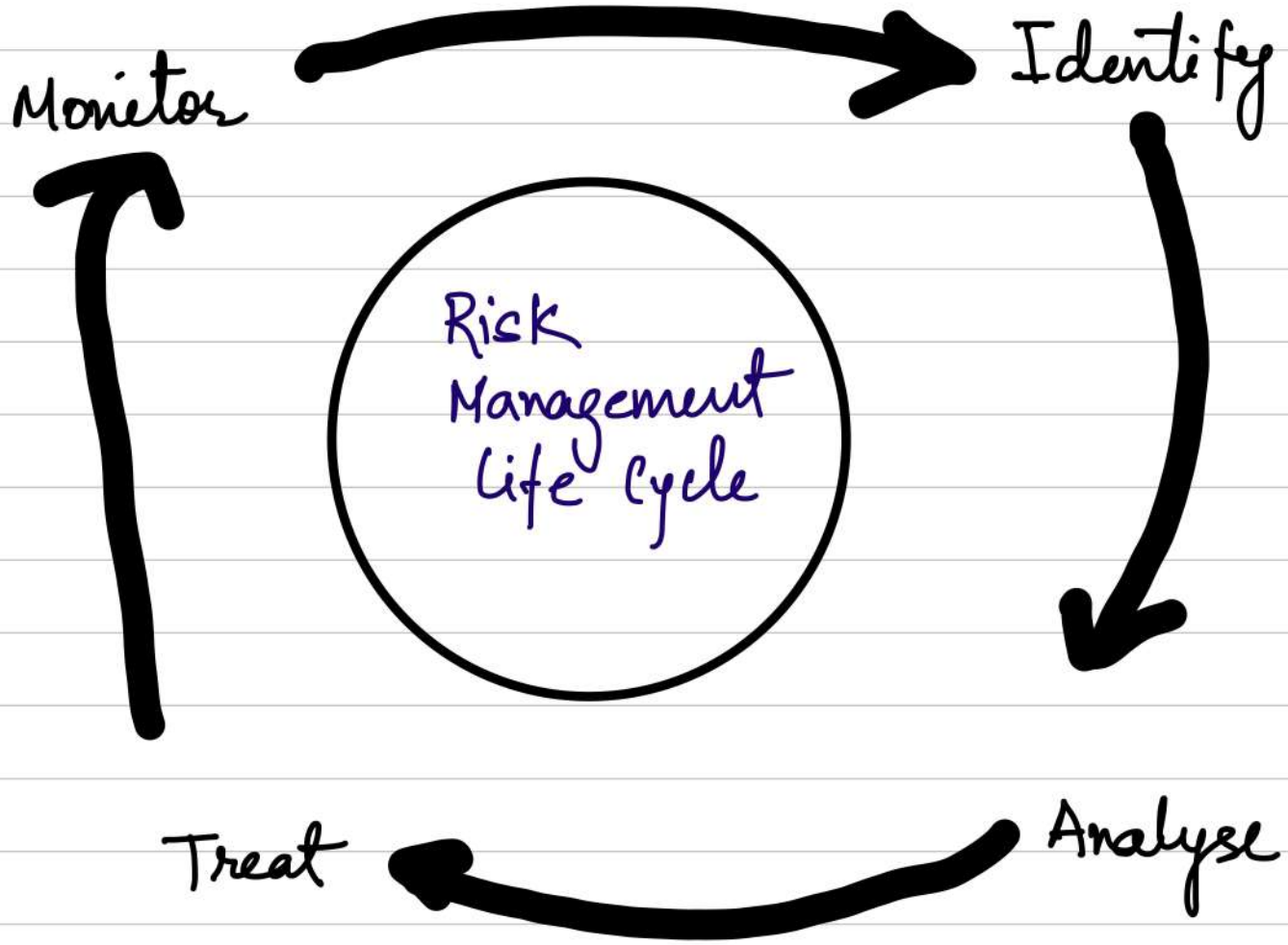
Identify Risk :-

- **Create System component categories** → understand the structure and identify dependencies.
- **Plan and Organize Process** → structure plan to execute the risk manage process effectively.
- **Develop Inventory Of Assets** → list of Assets, include physical, digital, and human resources.
- **Identify Threats** → list potential threats that impact the system or Assets.
- **Specify Vulnerable Assets** → Identify assets that are most susceptible to specific threat or vulner.
- **Assign value or Impact Rating** → Evalute the criticality of Assets based on C.I.A.
- **Assess likelihood for Vulnerabilities** → Determine the probability of threats exploit vulner
- **Calculate Relative Risk Factor** → combine asset values, impact ratings, and likelihood assessment.

Preliminary Review → Identify potential measure or safeguards to mitigate risk.

Document Findings. → Records all Finding, include risk calculation, identified vulnerabilities, and proposed controls.

Risk Management Life Cycle:-



Asset Classification

1. Physical Assets :- Infrastructure assets, Computer System.
2. S/W Assets :- Media
3. Information Assets :- Shared Folder, Hard copies.
4. Service Assets :- security & house keeping service, IT helpdesk.
5. Human Resources :- VP's, Manager, Associates.

Asset Grouping :-

1. Information :- Data and Documents.
2. S/W Assets :- Application S/W, system S/W, development tools, utilities.

Asset Valuation :-

↳ It is dependent and derived from :-

C → confidentiality.
I → Integrity.
A → Availability.

Asset Value (AV) Determination

↳ Addition Method : $(C+I+A = AV)$

↳ Multiplication Method :-

$(C * I * A = AV)$

↳ Aggregated Method :-

$$\frac{(C+I+A)}{3} = AV$$

Ranking :-

↳ Critical.
↳ High.
↳ Medium.
↳ low.

Risk Assessment :-

Step 1 :- Identification of Threats.

Step 2 :- Associated Vulnerabilities

Step 3 :- Determination of Impact

Step 4 :- Determination of likelihood.

(1) Threat Identification

- Potential Vulnerabilities.
- Existing control.
- Past History.

(2) Vulnerability Assessment :-

- Weakness / flaw
- Identification
  - Source of threat.
  - Threat Action
  - Audit Report
  - Past Assessment Report

(3) Impact Determination

↳ Individual Asset value and Exposure rating.

↳ loss of C.I.A

Impact Matrix :-

Rating	Consequence	Definitions
1.	Insignificant	Minor security breach, last for several days.
2.	Minor	Security breach in one or more area, last this less than 1 week.
3.	Moderate	Limited systemic breach, last up to 2 week.
4.	Major	Ongoing systemic breach, last 4- 8 week.

(4) Likelihood Determination

↳ It indicates the probability that potential vulnerability may be exploited.

Likelihood Matrix:—

Rating	Likelihood Description	Definition
1.	Rare	occur exceptional, very unlikely.
2.	Unlikely.	could occur at sometime
3.	Possible	Might occur, difficult to control, external influence.
4.	Likely	well probably occur. not be suprised.
5.	Almost Certain	Expected to occur, certainly sooner and later.

Risk Determination :-

↳ Assess the level of risk to the system.

↳ Point to consider :-

↳ Likelihood, Magnitude, capability, and collection of various components.

↳ The matrix is used to determine the relation.

RD = Matrix [Likelihood, Impact]

Likelihood \ Impact	Dooms Day	Catastrophic	Major	Moderate	Minor	Insignificant
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Determination Level

Risk level	Mitigation
Extreme (E)	Research and Management, executive / director level planning, Monitoring required.
High (H)	Require Management attention, Planning senior Project or team leads.
Medium (M)	Managed by existing specific, Monitoring and response
Low (L)	Manged by Routing Procedures.

Threat Agent and Elements

Agent :—	Elements
(1) Accidents →	Fire, Smoke, structure / Building.

(2) Criminal Activity → Personal Assault, Vandalism.

(3) Sabotage → Tempering, Data manipulation / Theft, Malicious Insider.

(4) Terrorism :- Bomb, Explosion, Kidnaping, Attack.

(5) Information warefare :- Malware, Dos, Exploit, Ransomware N/W Eavesdropping.

(6) Civil Unrest :- Riot, looting.

(7) National Disasters :- Earthquake, Flood, storms, Fires, Avalanche.

(8) Conventional Weapons :- Missiles, Rockets, Bombs, Gun.

(9) Weapons of Mass Distruction :- Nuclear, chemical, Radiological, Biological.

Case Study :—

↳ There is an war like scenario, you have to calculate the impact, likelihood, Risk level, and Risk determination on travel, Personnel, and Assets.

Solution :—

① Impact Matrix :—

	Travel	Personnel	Assets
Dooms Day	complete distruction close of more than year.	No one Alive	100% loss
Catastrophic	complete disruption close for 6 months,	Mass Casualties	85% loss
Major	widespread disruption, close for > 3 months.	Severe injuries.	65% loss
Moderate	significant disruption, close for > 1 months	Serious but non-life threatening	45% Major Damage.
Minor	Minor Disruption, close for > 1 weeks	Minor injuries	Minor Damage 25% loss
Insignificant	No disruptions, minor delays, close for some hours.	No Injuries	5% Damage.

② Likelihood Matrix

	Probability	% Guidelines	Expected Frequency
Almost Certain	Expected	> 90%	Near Daily or week
likely	High	60 - 90%	week to month
Possible	Reasonable	30 - 60%	month or Year
unlikely	unrealistic	5 - 30%	year or decades
Rare	Doubtful	< 5%	Never.

③ Risk level

	safety & security	Travel Disruption
Extreme	Extremely Dangerous. unpredictable security Risk	Chaotic, travel impossible
High	Can be Dangerous. unexpected security Risk	Travel is possible, but Potential, widespread disruption.
Medium	Not completely safe Predictable security risk	Travel is possible, but there is a potential for disruptions.

Low	Safe with few Security risk.	Travel is possible with a routine disruption

(4) Risk Determination Matrix

Impact / Likelihood	Doomsday	Catastrophic Major	Moderate	Minor	Insignificant
Almost Certain	E	E	H	M	L
likely	E	E	H	M	L
Possible	E	H	M	L	L
unlikely	M	M	L	L	L
Rare	L	L	L	L	L

Social Engineering

→ To manipulate people by deception.

→ Taking out information perform an action.

It captures two Outcomes

① Direct loss of Information.

② Achievement of Action desired by the Attacker.

Attack Cycle

↳ Social Engg has four Attack Vector.

(1) Research :- (i) Collecting as much information about victim.

(ii) Info used for targeted attack.

(2) Developing Trust :- In this phase the victim trust the attacker.

(3) Exploiting Trust :-

↳ Exploitation Phase.

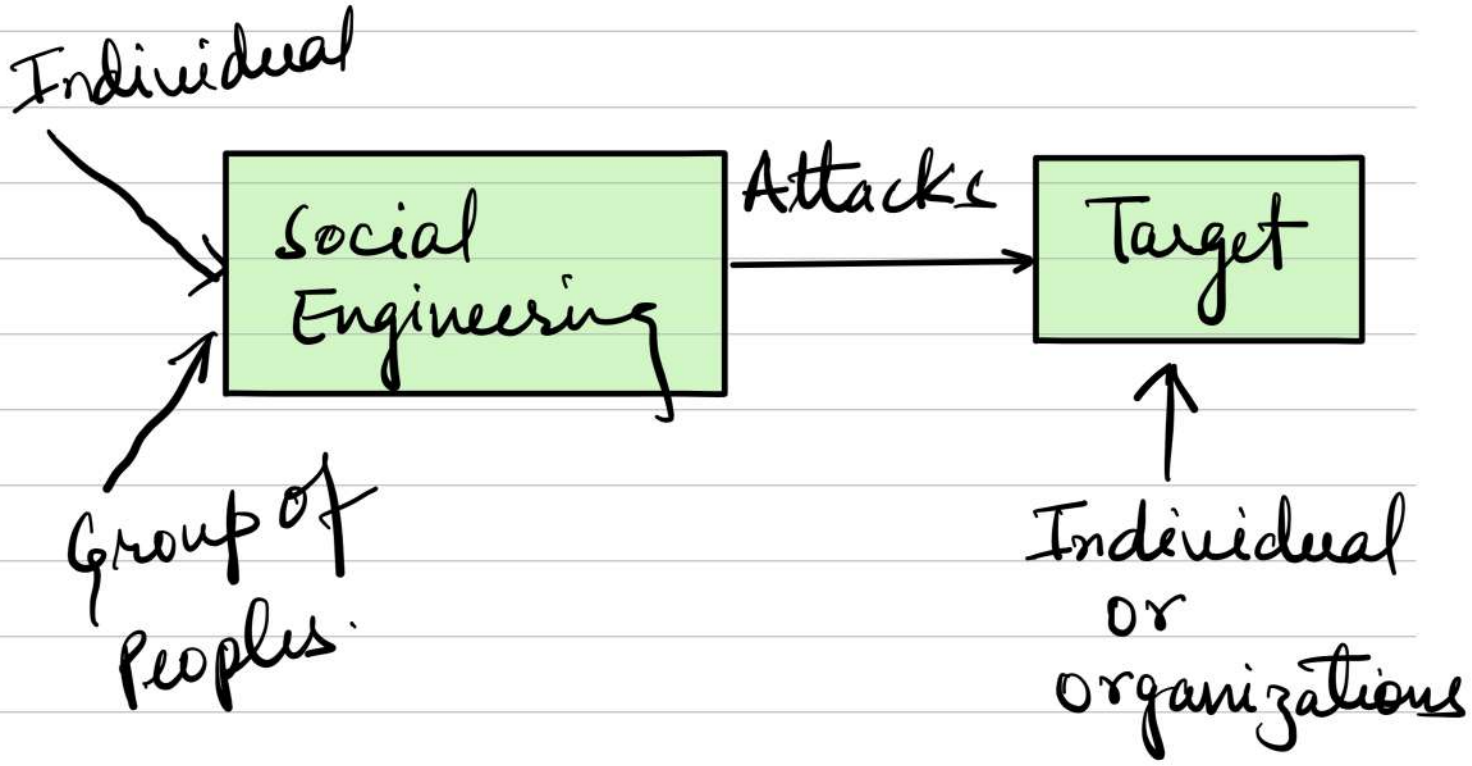
↳ Measurable gain in info or privileges is achived by the attackers.

(4) utilize Information

↳ Final Phase, which is

Cashing the previous phase info.

Basic Architecture



Social Engineering Technique and Primitives

1. Phishing
2. Pretexting
3. Baiting
4. Dumpster Diving
5. Shoulder Surfing

Medium

1. Email
2. Face to Face
3. Telephone
4. SMS
5. Paper Mail
6. Storage Media
7. Web pages
8. Pamphlets

Goals

1. Financial Gain.
2. Unauthorized Access.
3. Service Disruptions.

Framework Of Social Engg:-

1. Attack Formulation
   - ↳ Define Goals / Plan.

(2) Information Gathering

↳ Identify.
↳ Gather Information.
↳ Access Information.

(3) Preparation

↳ Combination And Analyses.
↳ Development of an Attacks.

(4) Develop Relationship

↳ Establishment of communicatio
↳ Build Positive Relationship.

(5) Exploit Relationship

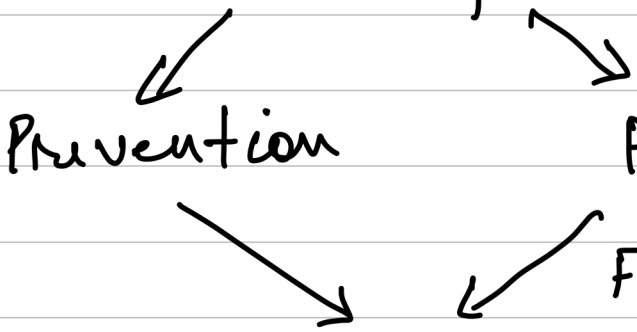
↳ Priming Target :- Manipulate victim Emotion.

↳ Elicitation :- Favor from the victim.

(6) Debrief

- Maintenance
  - Attack take Place exploit extreme emotion.
- Transition
  - Attackers decide whether the attack is achieved.
    - or restart complete phase.

Why Physical Security?



Facilities like (Officies, Houses, Hotels, Army.)

Define Physical Security?

↳ It concerned with active and passive measure.

↳ It is design to prevent unauthorized access to devices / systems.

↳ It safe against the threats such as terrorism, damage, criminal.

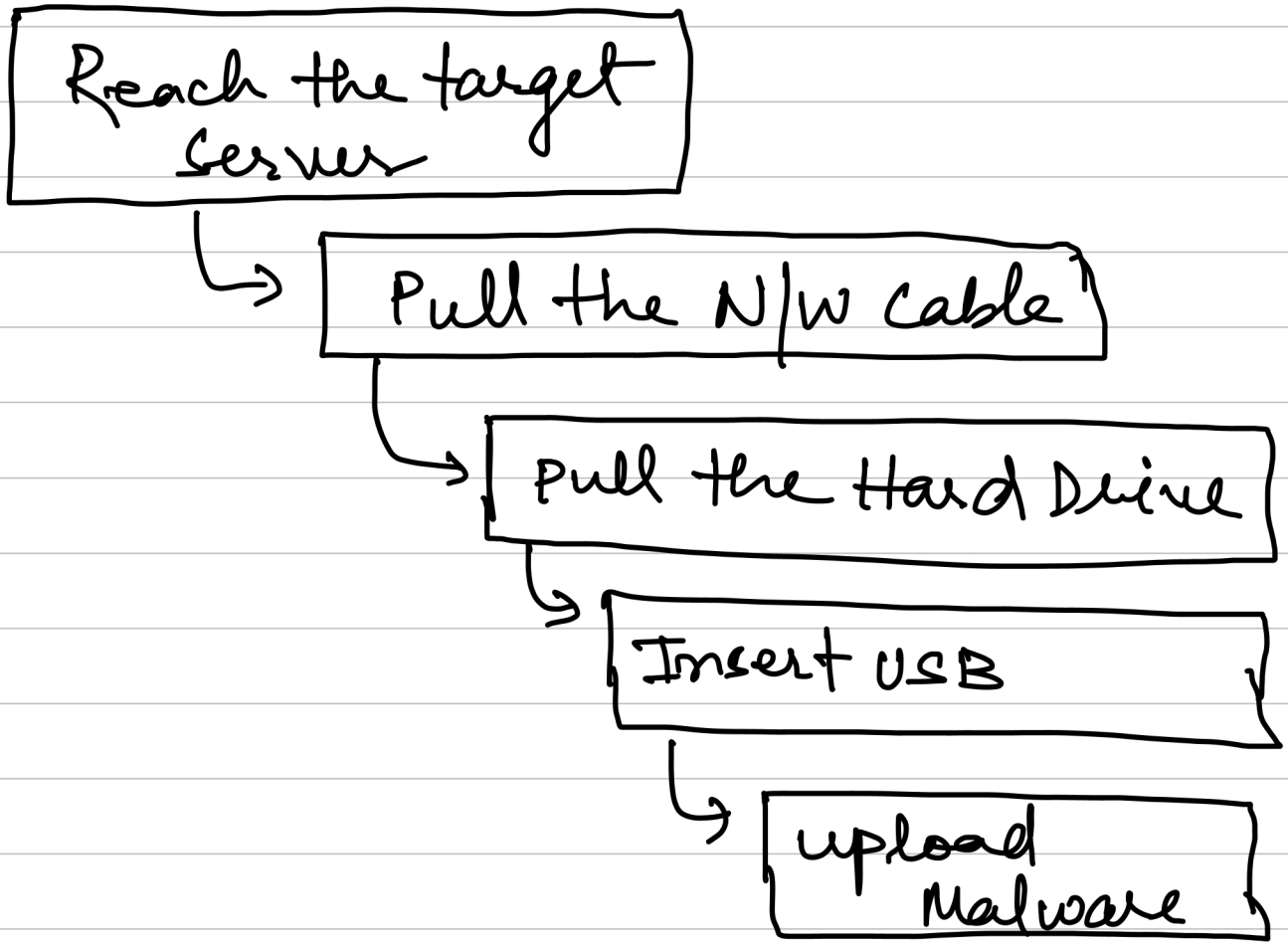
Historically:- To defend Attack we use

Guards / Locks / Alarms

Now :- we defend Attack because :-

↳ Biometrics / CCTV / Hire Hackers.

Example :- If you want to access to data center.



Approach to Physical Security :-

↳ understand the requirement & organization Features.

↳ Determine threats & conduct Risk Analysis.

↳ Meet stakeholders (to determine the risk).

↳ Suggest counter measures for protecting the organizations

↳ Align and Integrate existing systems and process.

↳ Perform Impact Analysis.

↳ Review Risk.

Threat Types :—

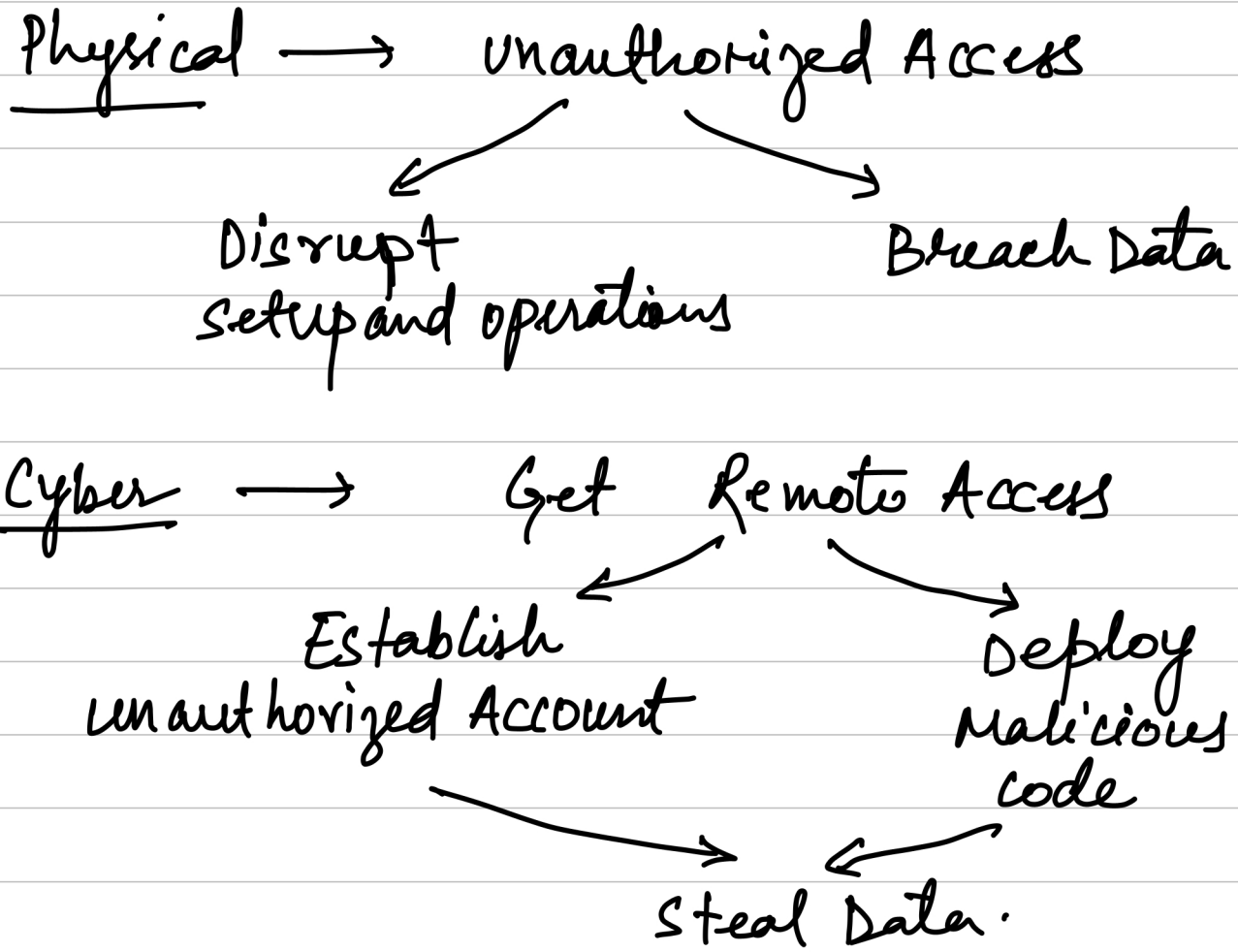
① Man-Made :— Explosions / unauthorized Access / Emp Error / Process.

② Politically Motivated :- Riots / Strikes / Bombing / Terror Attack.

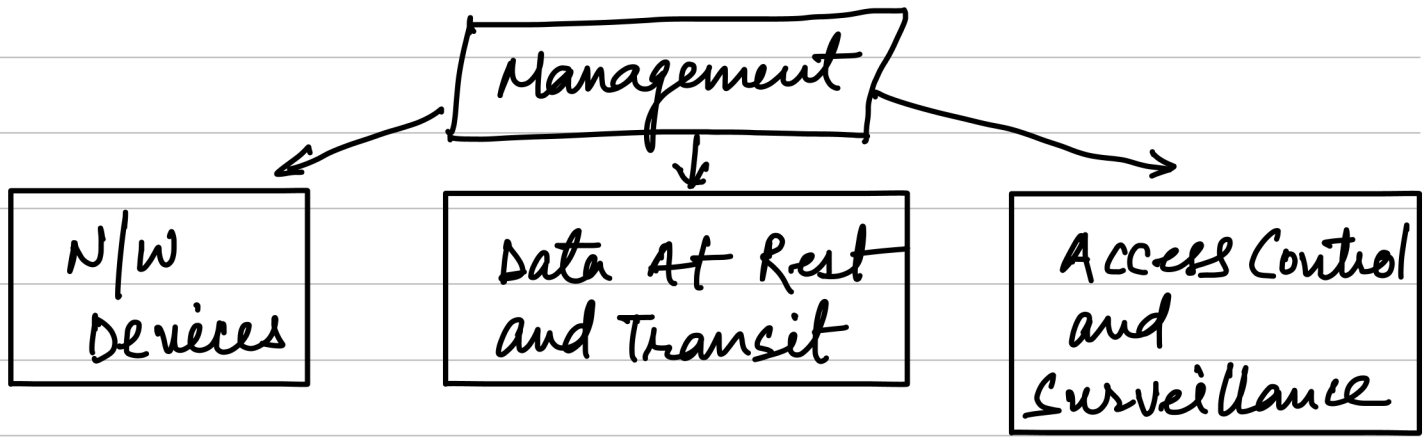
Issuess Related to Physical Security

- Tailgating
- Unauthorized Access using USB and N/W Ports.
- Data Center / Server room Access
- Unsecure end point devices connected to LAN.
- CRB (Chemical / Biological / Radioactive)
- Plant Explosives (Bombs
- Social Engg
- Stealing (Dumpster Diving / Disk / Devices / Access key)

Relationship b/w Physical and Cyber Security



Convergence between Cyber and Physical



Governance

- Best Practices.
- Mitigate Theft.
- Increase Monitoring.

How to Implement :-

- Technology.
- Policies.
- Economics.
- Staff.

Layer of Physical Security

- Design.
- Detection.
- Identification.
- control.

① Design :- "Structure Design" → limit entry/exit movement.

mitigate limit Attack block Access

How:- Fences / Wires / speed Breakers / Walls / Door / Gates / Lobbies / Bunkers

(2) Detection:- (Difficult to block but we take measeure to find Attack.

↳ we use:- Motion Sensor / Lights / Cameras / Human Guards.

(3) Identification:-

↳ Ensure authorized Access (Facility Area)

↳ we use:- Retina Scan / Finger print / Voice / Digital Signature / Id Card.

(4) Control:- Limit Access to Seceure Area.

↳ we use:- Electronic / Mechanical / Procedeal

↳ lock-code on doors / check point / Electronic Access Point / Key lock Door.

* What is Physical Security Control ?

1. Security in layers
2. Technical Control
3. Environmental & Power Control
4. Logging Control
5. Perception as Physical Security.

1. Security in layers :- Physical Security

1. outer layer
2. Inner layer.

1. outer layer :-

1. Facility Aspects :-
   - Location
     - City / Mall / shop / outside City
     - Jungle / Remote
   - Types
     - office / shop Factory, university / warehouse /
     - Army / Defence Base /

② Element of Outer Layer

(i) Natural Barriers :-

↳ water body / hills / rock on one side.

(ii) Structural Barriers :-

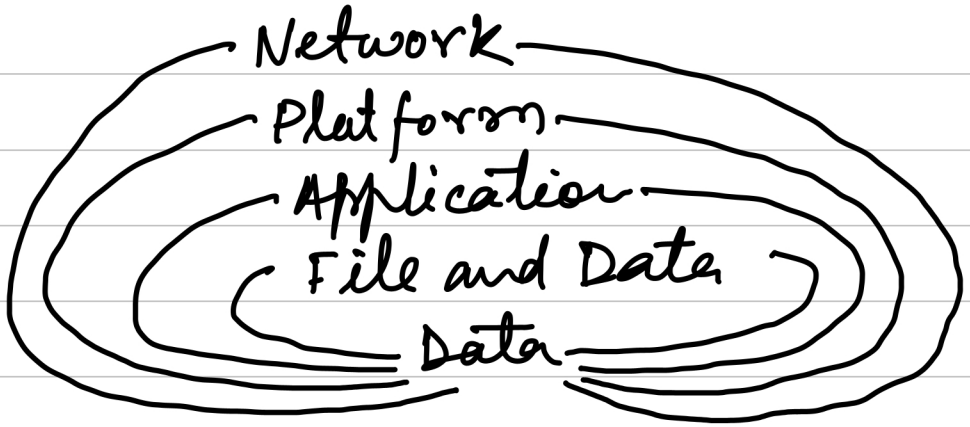
↳ man-made / implemented Fences / walls / Gates.

② Inner Layers :-

↳ Apply inside the building facility

↳ Use :- lock / Keys combinations / Patrols / Guards / CCTV

Cyber layers of security :-



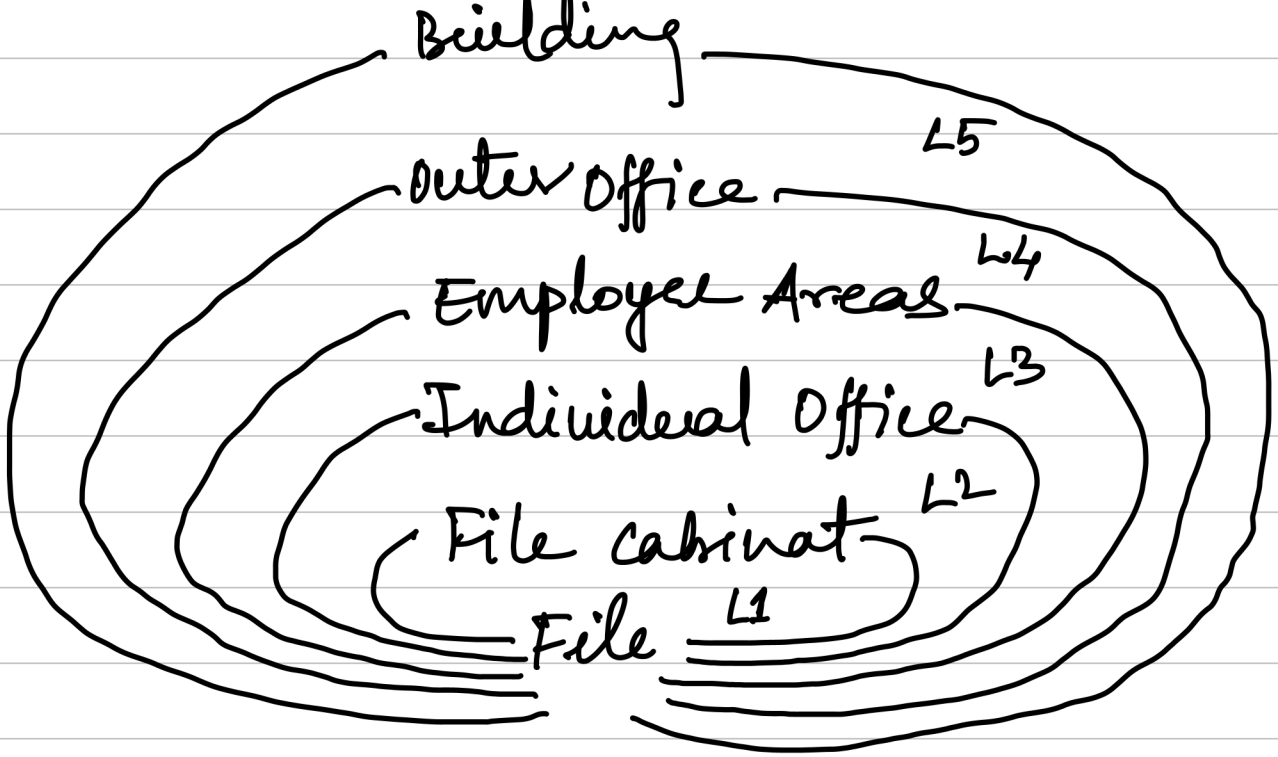
Network :- Firewalls / Data loss Prevention / Demilitarized Zones / Id Management, Traffic

Platform :- Antivirus / Patching / security specifications.

Application :- Secure Coding / Testing

File and Data :- Encryptions / Enterprise right Management.

Example :- Data security In building



② Technical Control :-

↳ Man Trap :- Authentication + Identification and High Secure Area.

↳ Turnstiles :-

↳ control / entry / exit

↳ Crowd control / Loss Prevention / Access Control.

↳ Biometrics :-

↳ Retina / Fingers / Facial.

↳ CCTV :-

↳ video Record / cameras / cam cordars / Motion sensor camera.

③ Environmental & Power Control

↳ ① Environmental Monitoring :-

↳ Heat (H) / ventilation (V) /

temp / Humidity / Air condition (AC)

↳ Power System :-

↳ AC / DC provision / power condition / Backup (UPS - Battery / solar).

↳ EMI shielding :-

↳ Faraday Cage.

↳ circuit overload, spikes.

↳ Fire Suppression :-

↳ Pull (P), Aim (A), Squeeze (S) sweep (S) procedure.

Type of Fire :- There are five types of Fire.

Type (A) :- "Ordinary combustibles"
("Ash")

↳ wood / Paper / Plastic / cloth / Rubber.

Type (B) :- "Flammable liquid and Gases"
("Barrel")

Liquid { Petrol / Diesel / oil-based Paints / Car-bike oil / Alcohol

Gases {
- Hydrogen :- party ballons
- Butane :- Cigratte Lighters
- Methane :- Cooking and hot water Syetem
- Ethylene :- Agricultur Industry.

(current)
Type (C) :- "Electrical Equipment"

↳ Circuit breakers / wiring / Appliances / Machinery.

(Dynamite)
Type (D) :- "Combustible Metals"

↳ Magnesium / Titanium / sodium / Potassium.

(Kitchen)
Type (K) :- Oils and Fats

↳ cooking oil / greases / fats.

↳ Electromagnetic and Electronic Locks :-

↳ Lock Picking :- manipulated / Tempered.

↳ Drilling :- Inoperable.

↳ Magnetic Locks:—

↳ utilize force of magnet.

(4) Access Logs / Audit Trails

↳ For review of Incident

↳ Date/Time, Entry/exit event, Emp Id, Failed Attempts

↳ it is not use for prevention

↳ It is used for investigation and detective

↳ Lower the vulnerability

↳ No immediate Action.

(5) Perception as Protection :-

↳ Develop mindset of security.

↳ Approaches :-

(1) Visible with real protection :-

↳ Guard / Roadblocks / Signs.

(2) Not visible with Real Protection :-

↳ CCTV (hidden)

(3) Illusion incorporated as Protection :-

↳ New MAC :- Set new password.

↳ Leaving Emp machine check.

↳ Buy a gift giving your credit card.

Security Containers / Storage Area security

Security Standard for Containers

- GSA (General Service Administration)
  - Developed in 7th July, 1949.
  - By Harry S. Truman.
- Aim:- streamline the work Federal goverment.
- It ensure Integrity and confidentiality of Assets.
- It is used to safeguard weapons, electronics, drugs, metals, money, files, etc.
- GSA maintain the standard
  - Class (1, 2, 3, 4):- obsolete and newer manufactured.
  - class (5, 6):- security containers and filing cabinets.

Use of Storage Containers :—

↳ Design, source code, configuration, components, Equipment, funds, valuable, weapons.

↳ GSA classified the container as per the "Resistances Against" in terms of "min/hours".

Category	classification
• Forced Entry	How many mins.
• secret Entry	Sneaking / stealth / Secret.
• Lock Manipulation	manipulate lock without original key.
• Radiological Attack	The elements like 113 Uranium, Iridium 192 cobalt-60, Radon Gas, Potassium-40 harm.

Containers class:- "man hours" (mh)
"man minutes" (mm)

	class 1	class 2	class 3	class 4	class 5	class 6
Forced Entry	20 mm	5 mm	none	5 mm	10 mm	none
Secret Entry	20 mm	20 mm	20 mh	30 mm	30 mh	30 mh
Lock manipulation	20 mh	20 mh	20 mh	2 mh	20 mh	20 mh
Radiological Attack	20 mh	20 mh		20 mh	20 mh	20 mh
wheels	Non metallic	metallic			mettalic	

Critical IT Security Terms

↳ (AVT)

Asset (A) :- Protect

↳ People, property, Information
(Emp) (Tangible) (Document)

Vulnerability (V) :- weaknesses or gap on protection.

Threat (T):- Threat is to protect against.

(malware, phishing, Social Engg, Internal Agent)

Attack:- (T+V)

↳ Someone follow the threat and vulnerability.

Countermeasure:-

↳ Mitigation plan to address vulnerabilities

Risk:-

↳ Intersection of Assets, Threats, and vulnerabilities

$$R = A + T + V$$

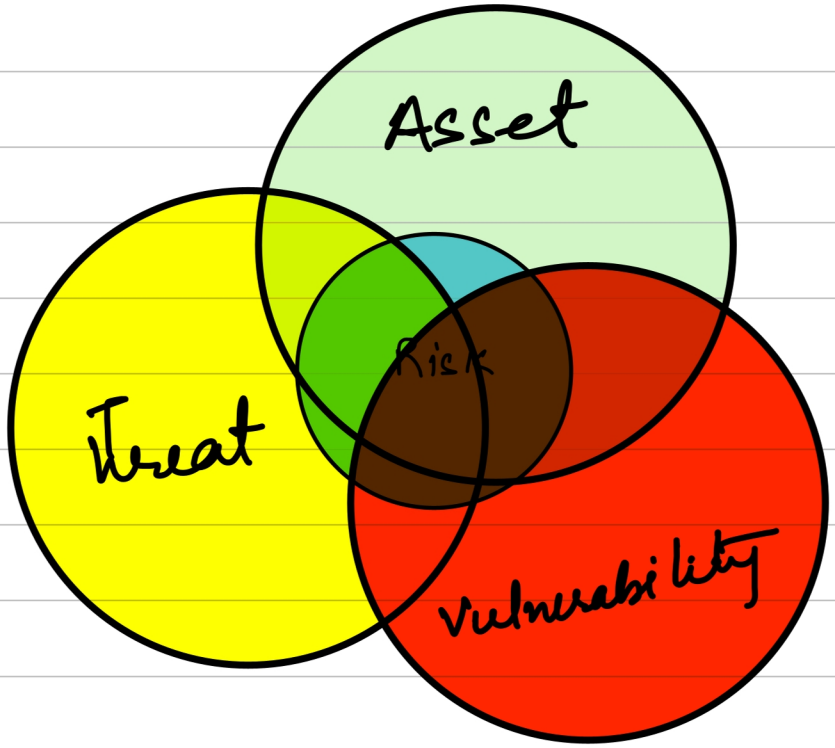
Risk:- Business Disruption, Financial losses, loss of privacy, Damage to reputation, loss of confidence

legal Penalties, Impaired Growth, loss of life.

Threat :- Angry Emp, Dishonest Emp, Criminals, Goverment, Terrorists, Hacker, Nature, competitors.

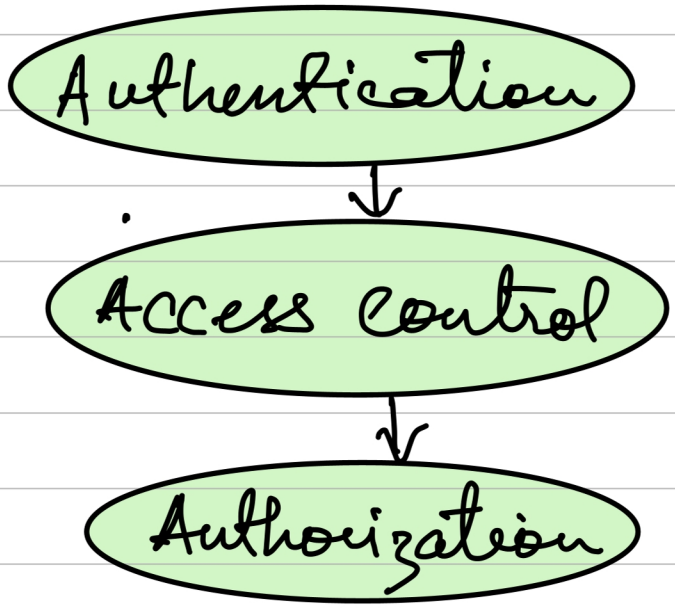
Vulnerability :- S/W bugs, Broken processes, Ineffective control, H/W Flaws Business change, legacy Systems, Inadequate BCP, Human Error.

Asset :- Server Machines, PC & laptop, Mobile Devices, IT N/W, S/W & Apps, Data & Info, connected Devices, Wearable Devices, Physical Infra.



Access Control :-

↳



* use various technology :- Password, PII, Biometrics, Scans, Physical/Electronic / Keys / Badges / Cards.

* Password :-

- Strong Password
  - Long Password (12-16 character)
    - Mix of character
      - uppercase
      - lower case
      - Integer / Number
  - Avoid common words / pattern
  - use passphase (random word)
  - Use unique Password for every Account
    - Use Password manager
      - Bitwarden, 1Password, LastPass.

Scan :-

↳ Human Scan :-

Detect metal, Explosive weapons

↳ walk-Through Metal Detectors (WTMDs)

↳ Full-Body Scanners

↳ use : (Millimeter wave & Back scatter X-rays)

↳ Handheld Metal Detectors

↳ Pinpoint specific items

↳ Bags & Cargo

↳ X-ray

↳ Explosive Detection System (EDS)

↳ Computed Tomography (CT scan)

↳ Canine Unit → Trained Dogs.

↳ Liquid & Chemical Scanning :-

↳ Liquid Scanners :- Analyze composition of liquid.

↳ Chemical Trace Detectors :-

↳ Trace the explosive substance on luggage or cargo.

Biometric Authentications :- (Identify Physiological or Behavioral characteristics)

① Facial Recognition :-

↳ Analyze the Face features like (size and shape of eyes, nose, and mouth).

↳ Create the template (used for matching with stored template).

where we use ↳ Surveillance system, Border control, and smartphone)

(2) Fingerprint :-

↳ Capture unique patterns of ridges and valleys

↳ use optical sensors to capture high-resolution images.

↳ use :- smartphones, laptops, Access control systems.

(3) Voice Authentication :-

↳ Identify (pitch, tone, and speech patterns)

↳ create the voice prints for matching.

use. ↳ Telephone banking / voice controlled devices / Remote Access systems.

(4) Eye Scanning :-

↳ iris recognitions and retina scanning.

↳ Iris scanning find the patterns of Iris

↳ Retina scan captures the unique blood vessel patterns.

↳ Iris scan is widely used due to ease of use.

(5) Face Authentication :-

↳ capture active users participation.

↳ Such as :- Nodding / blinking

↳ Prevent spoofing Attempts.

(6) Handwriting Identification

↳ Analyze strokes and nuances in handwriting.

↳ Examine stroke and pen pressure, letter formation.

↳ use :- Document verification and forensic Analysis.

(7) Palm Recognitions :-

↳ Identify the patterns of lines, creases, and ridges.

↳ optical sensors to create palmprint.

Use :- ↳ Access control system and time attendence systems.

Personally Identifiable Information (PII)

Any data ↳ utilized to identify or distinguish individual:

(1) Voice data :- Authentication + Identification

(2) A/c Number :- Bank A/c number or credit card number.

(3) Vehicle or license :- The details link with the individuals. To control the identity theft or fraud.

(4) Biometric Identifiers :- Behavioral attributes enable individual identification. To control the unauthorized Access or misuse.

(5) Name, address, Social Security and Birthdate :-

↳ The info is used to identify the individual uniquely.

↳ Used for :- Registration, identity verification and communication.

(6) Medical & Health Plan Info :-

sensitive ↳ Medical History, Health Insurance Info. Policy details, Treatment Record.

↳ Privacy Regulation like "HIPAA"

{ Health Insurance Portability And Accountability Act. }

(7) Full Face Photo :-

↳ used for :- Identification + verification.

↳ Identity Theft or misuse.

(8) Mobile, Email, Phone & Fax :-

↳ Info used for communication.

Secure the Info ↳ To preserve the individual privacy and prevent unwanted harassment.

(9) Geographic Information

↳ Location based data (such co-ordinates or street Address)

↳ Info Gather via Mobile devices.

Video Technology :-

↳ Type :- CAM's, CCTV, Digital CAM.

↳ use for :-

↳ collect evidence

↳ Detect and Record activities of intruders.

↳ Monitoring negligence of staff / employees.

↳ Take action on past/present incidents.

↳ Review (Policy and Process)

Framework For Video Surveillance

(1) Remote Site :- used to monitored Remotely.

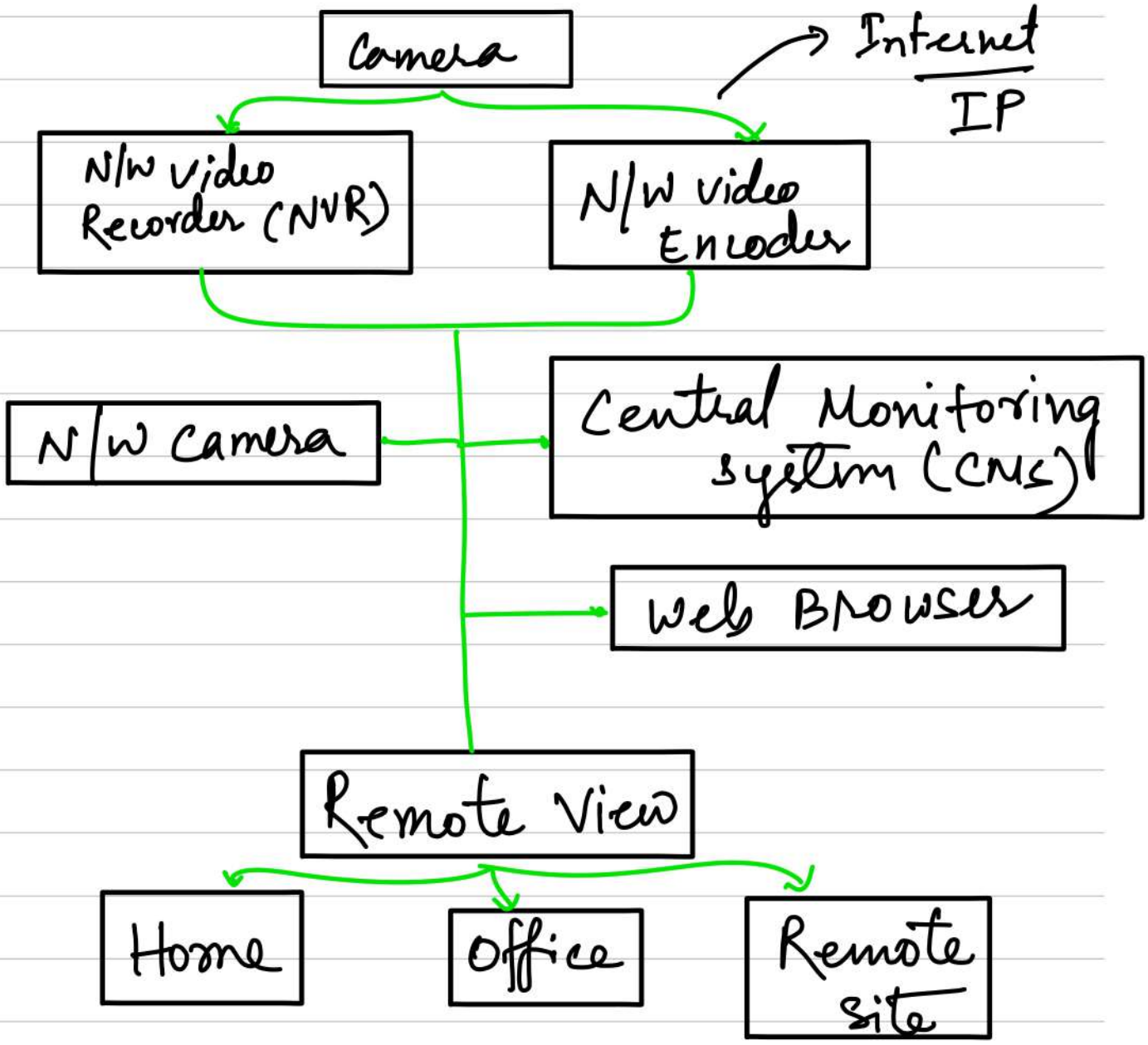
(2) Home :- Residential Properties Monitoring.

(3) Office :- workplace environment monitoring.

(4) Remote View :- Accessing Live or recorded footage.

(5) N/W Camera :- Connect directly to an IP N/W.

↳ Transmit videodata from cameras to monitoring stations.



Network Video Encoder :- Convert the Analog camera signal to digital signal.
↳ used for :- Storage and transmission.

Web browser :- View video footage via internet.

Central Monitoring System (CMS) :- Monitor and Managing multiple surveillance cameras.

PoE (Power Over Ethernet)

↳ Method to supply the power over the standard Ethernet cable.

↳ IEEE 802.3af divides PoE Technology into two distinct Parts :—

① Power Sourcing Equipment (PSE)
↳ supply power to the cable.

② Powered Devices (PD's)
↳ Accept Devices.

History of PoE :—

↳ First Applied by Cisco in 2000.

↳ Get support during 2001 - 2002.

↳ 803.2af defines voltage and Current ratings for transmission - 2003.

PoE Features :-

↳ Transfer Data and Power.

↳ No extension for existing Architecture.

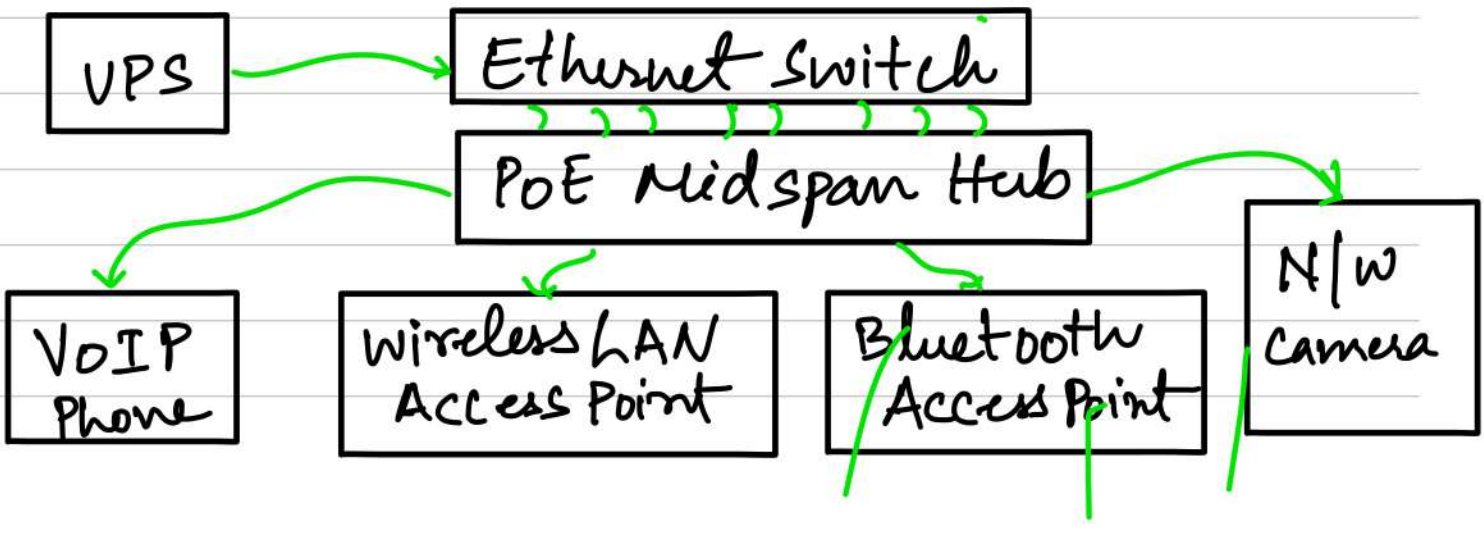
↳ Low Power loss over single cable Transmission.

PoE Specifications :-

↳ Send upto 15.4 W on cable.

↳ Max transmission of 100m before signal decay.

↳ support 10mb or 100mb ethernet connections for end devices.



Advantages:—

↳ One set of wires to bring to your appliance.

↳ Save money for expensive installations.

↳ Easy Movement of Equipments.

Disadvantages:—

↳ use SNMP (simple N/W Management protocol) to monitor and control.

↳ Appliances can be shutdown or reset remotely.

↳ Not ideal for High power applications.

PoE Pin Configuration

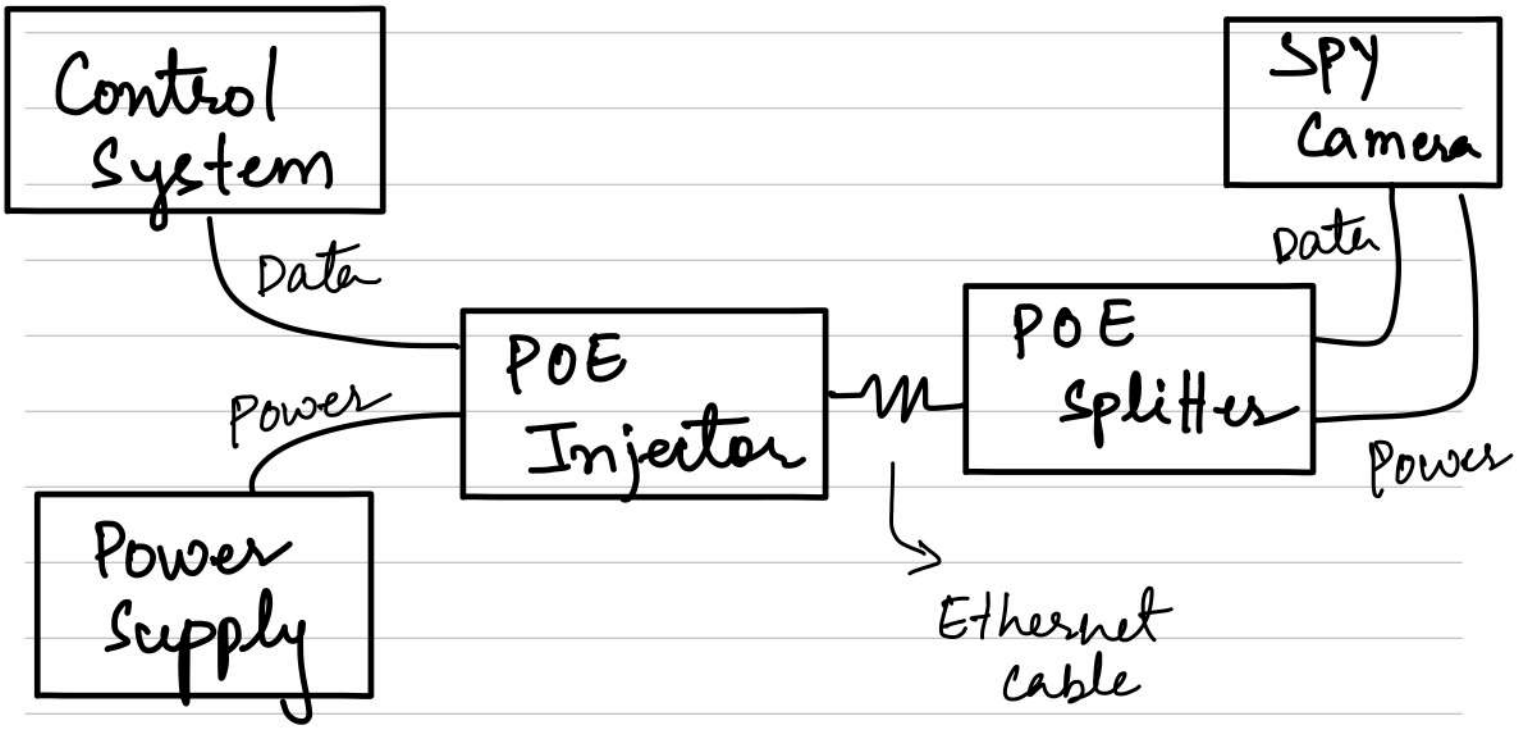
↳ color code :— ↳ T568A
↳ T568B

Pin	T568A	TB68B
Pin 1	White/Green stripe	White/orange stripe
Pin 2	Green solid	Orange solid
Pin 3	White/orange stripe	White/Green stripe
Pin 4	Blue solid	Blue solid.
Pin 5	White/Blue stripe	White/Blue stripe
Pin 6	Orange solid	Green solid
Pin 7	White/brown stripe	White/brown stripe
Pin 8	Brown solid	Brown solid

RJ45 - Plug (T568B)

Pin		
1. Data	———	1. Data
2. Data	———	2. Data
3. Data	———	3. Data
4. + DC	———	4. No connect
5. + DC	———	5. No Connect
6. Data	———	6. Data
7. - DC	———	7. No Connect
8. - DC	———	8. No connect.

How it works :-



PoE Injector :- Two input ports and one output ports.

Input = Ethernet + DC power supply

Output = PoE Ethernet.

PoE Splitter :-

↳ One I/P port and Two o/p ports.

Input = PoE Ethernet

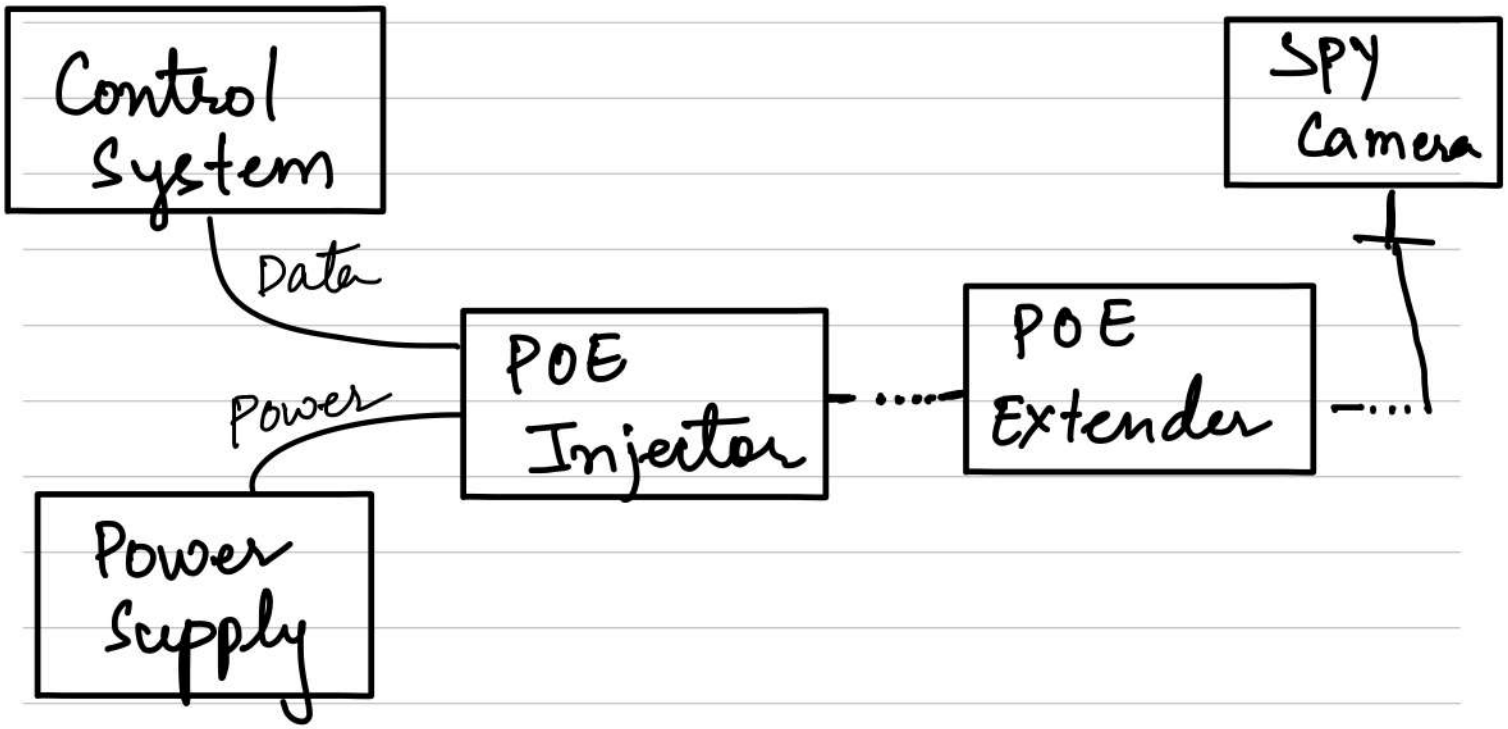
Output = DC power supply + Ethernet connection

PoE Extender :-

↳ It is used when the N/W span over large distances.

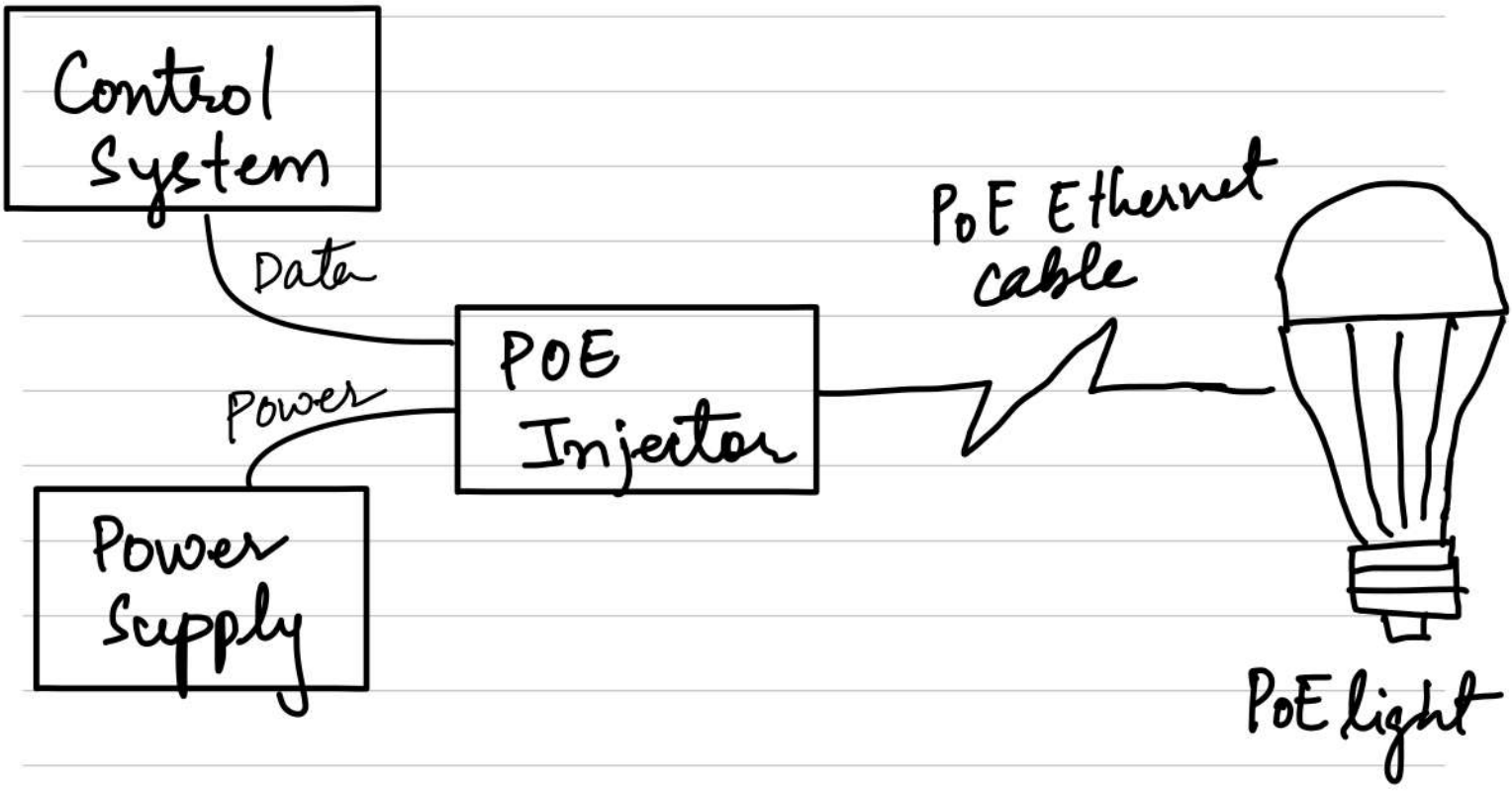
↳ Ex :- shopping Malls, Hotels, Offices,

↳ Apply at After 100m.



Block Diagram

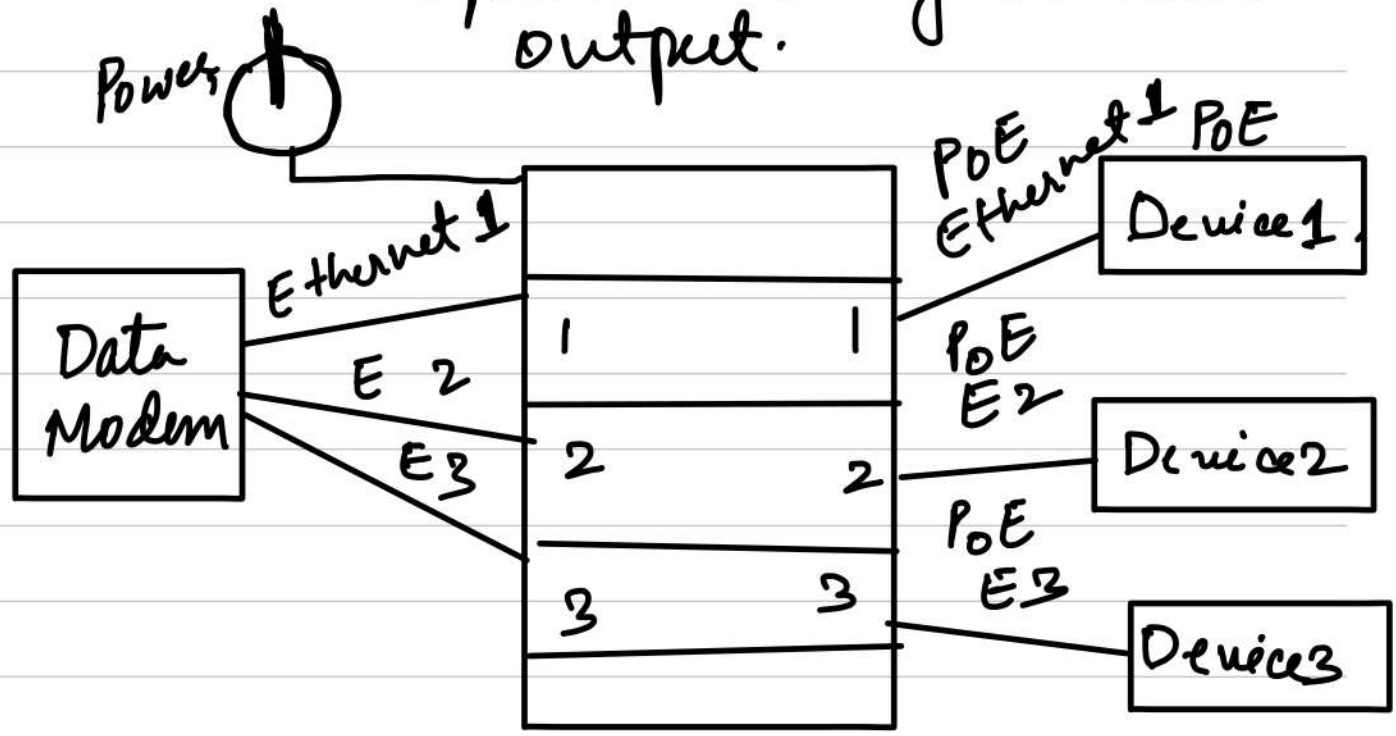
How PoE support Peripheral devices :-



PoE Hub :—

↳ It is similar to PoE injector.

↳ It take many ethernet connection and provide many Ethernet output.

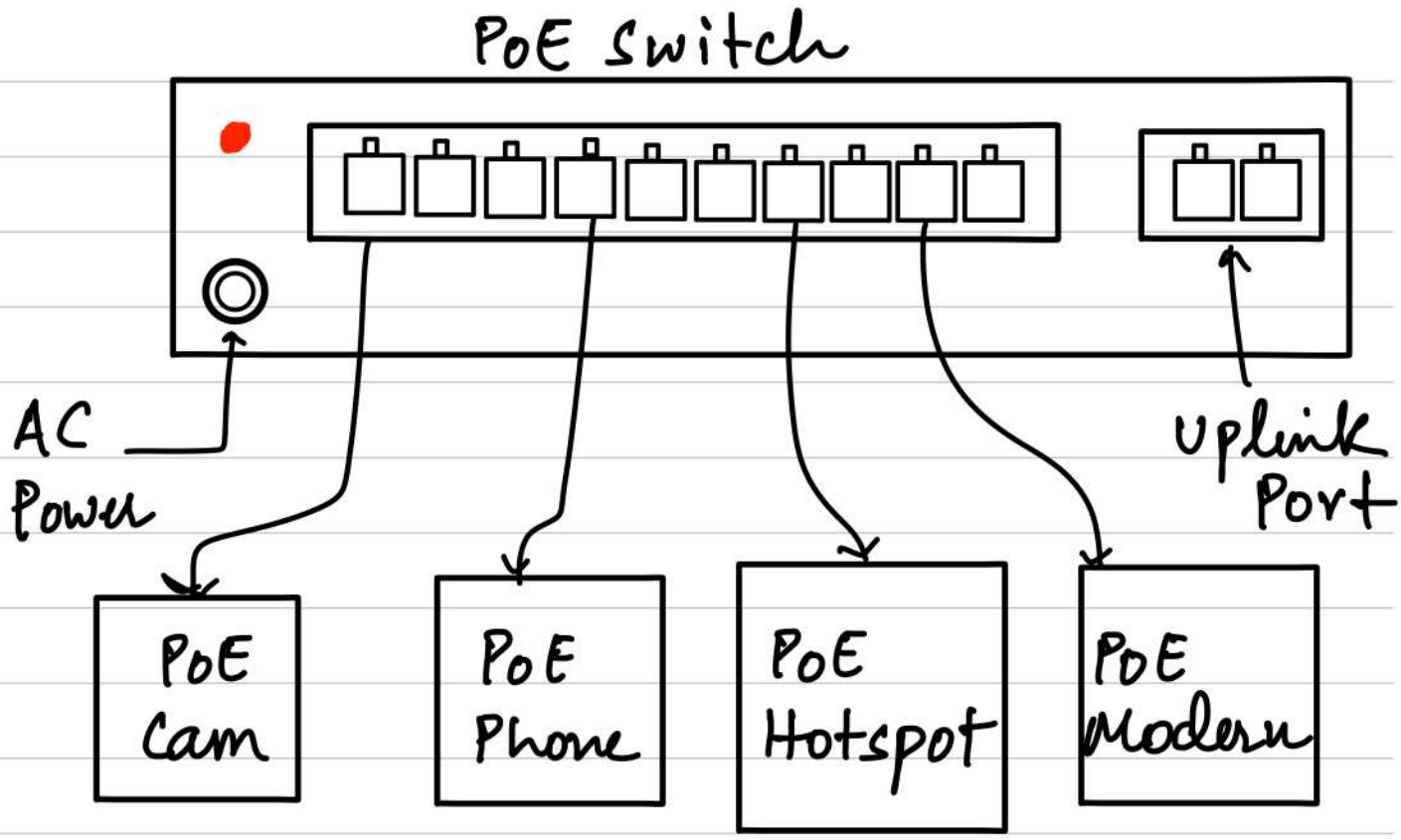


PoE Hub

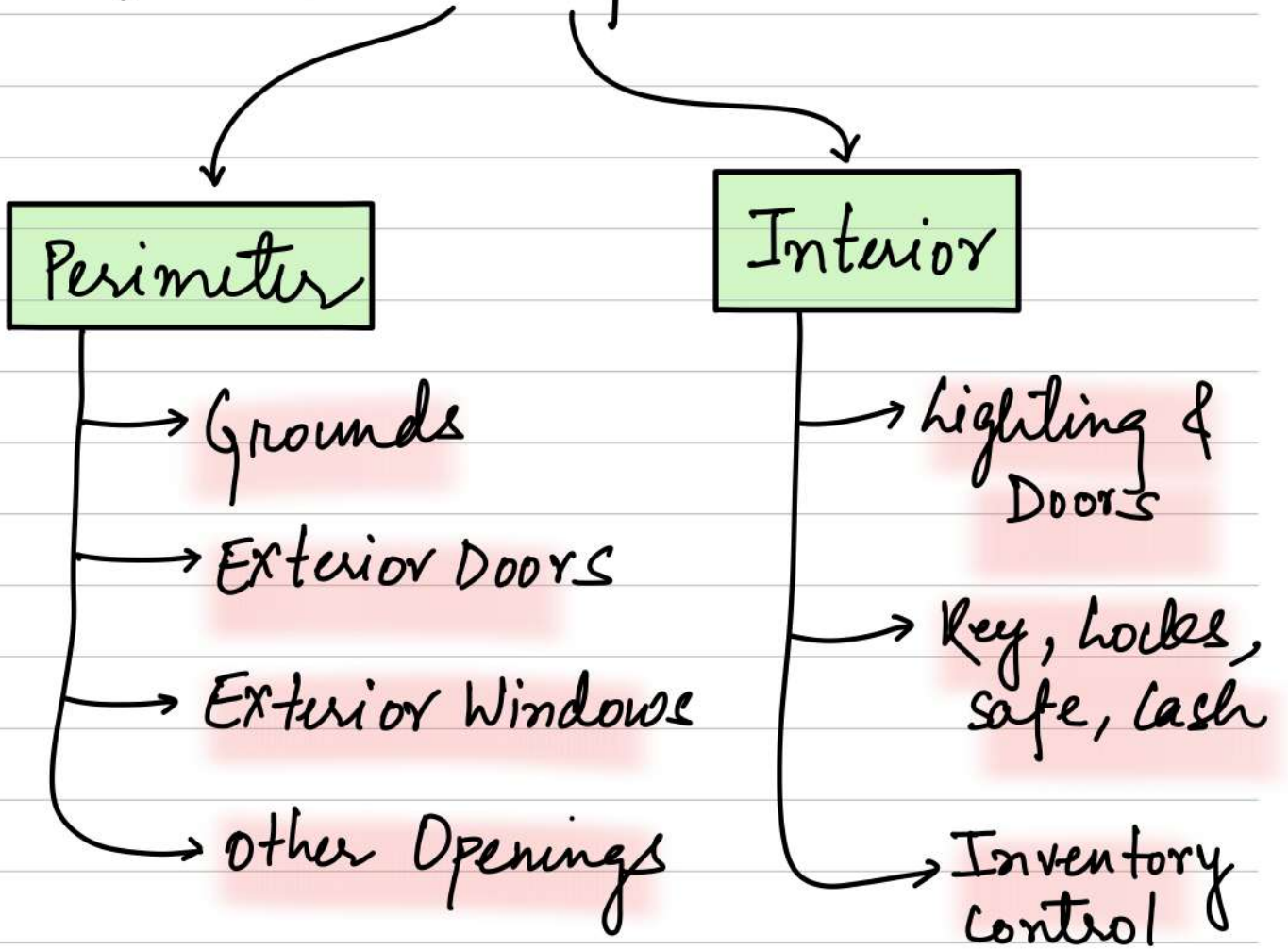
PoE Switch

↳ Provide PoE for each interface.

↳ It will work like port for connecting multiple PoE devices to single PC.


PoE Switch
AC Power
Uplink Port
PoE Cam
PoE Phone
PoE Hotspot
PoE Modem

Physical Security Checklist



Security of Grounds

- Fence/ Gates are Strong and Good condition.
- Distance b/w fence and building.
- Boxes/materials placed at safe distance.
- Remove weeds/ Trash

- Fence Gate hinges Secure and Non-Removable.
- Type of Locks and Chain to Secure gates.
- Eliminate unnecessary gates.
- Blind Area need to be protected.

Security of Exterior Doors

↳ Strong and Tough Doors.

↳ Hinges Pins located inside.

↳ All locks working Properly.

↳ Keys are in possession of authorized personnel.

↳ Keys are issued during on duty.

Security of Exterior Windows :—

↳ steel mesh/iron bar, bricks.

↳ All windows with 14 feet of the Ground.

↳ connected to Alarms.

↳ Vents having 1-Square feet.

Security of Other's Openings :—

↳ Manholes or similar openings that provides direct Access.

↳ Secure manholes or similar openings.

↳ Sidewalk door or gate (secure).

↳ Skylights area is protected with bars or Alam.

↳ Roof hatches properly secure.

↳ AC or vent protected.

↳ Fire exit or escapes route design secure.

Security of Interior :-

Lighting & Doors

↳ light must be adequate.

↳ Doors :-
- ↳ solid materials.
- ↳ Iron + wooden door.
- ↳ Door hinges install inwards.
- ↳ Atleast one lock on each door.

Keys / Locks / Safe / Cash

↳ Key control / register / system ? } Logs
↳ Master Keys ? } records.
↳ Loss of Key must report immediately.

↳ Doors are equiped with locks ?
↳ lock is working order ?
↳ lock location changed once a year ?

↳ lock combination changed on employee leaving.

↳ Safe is secure with alarm / visible from outside / changed regularly.

↳ Cash (Kept it minimum / not stored blank signed cheques / store at secure area).

Security of Inventory

↳ list all serial Numbers of equipment.

↳ check for missing or unaccounted item.

↳ Expensive business equipment present in surveillance.

Security Lighting

↳ Create intrusion Deterrance. (perception of security).

↳ use :- lamps, sensors, cams

↳ Level of light :-

↳ Bright / Dim / Darkness.

↳ Efficacy of light

↳ is measured in (lumens Per watt)

Types of lamps :-

① Incandescent :-

↳ use for Residence
↳ use filament for lumens.
↳ short life, costly.
↳ 10 - 20 LpW.

(2) Halogen :-

↳ use for automotive head lamps.

↳ work light hotels.

↳ It uses halogen gas. The gas allows the tungsten to burn hotter and brighter.

(3) Florescent :-

↳ Use the mercury vapor for luminescent.

↳ costly, and Generate 40-80 LpW.

↳ The mercury vapor produce ultraviolet light. It excites a phosphor coating to emit visible light.

(4) Mercury Vapor :-

↳ 30-60 LpW 'Or' 20000 hours.

(5) Metal Halide :-

↳ High Pressure Arc lamps.
↳ 80-100 LpW.
↳ High cost maintenance.
↳ Gas like Argon or Xenon used inside the tube.

(6) High Pressure Sodium :-

↳ Vaporized Sodium Metal.
↳ 100 LpW, Parking lots, Roads.
↳ low cost.

(7) low Pressure Sodeium

↳ 150 LpW
↳ very cost
↳ Maintain :- Street/Tunnels, Lab Exp.

Other Lighting Equipment :-

↳ Flood Light
↳ Mounted high/poles.

↳ Power lines are buried.
↳ Protective covers / switch box lock /
↳ Motion sensor internal / External

Alarm Systems :-

↳ (Perimeters / Area / Spot) protection.

Perimeter :-

↳ Door switches.
↳ Glass break detectors.
↳ Wooden screens.

Area :-

↳ Ultrasonic :- 23-26 Khz sound waves
5 to 40 feet.
↳ Microwave :- Vibrations, 0.3 - 300 GHz.
radio freq.
↳ Infrared :- It is passive, no signals.
↳ detect the object heat change.

Spot :-

↳ Proximity Detector :- Antenna to detect electrostatic field.

↳ Vibration detectors :-

↳ Sensitive microphones to detect the vibrations.

Security Personnel

↳ objective :-

↳ Keep eyes for Rule violations & Report to Authority.

↳ (Protect Assets / Goods / environments / Services)

↳ Types :-

↳ Personal / Private Security.
↳ Armed Security.
↳ Corporate Security.
↳ Residential Security
↳ Goverment Security
↳ Static Security.
↳ Mobile Security

Executive Protection

- VIPs protection.
- Plans:-
  - Home security
  - Armored vechiches.
  - Vehicle scrambling
  - Travel by private jets
  - 24x7 bodyguards.

Role and Responsibilities

1. Prevent :- Identify risk and try to mitigate.
2. visibility :- Be noticeable to discourage malicious Attempts.
3. Vigilance :- watchfull eye for abnormal activities.

Observe and Reports

- what / where / who / when.
- Alert / calm mind / log incident.

Q. what are the Functioning of security

1. Training
2. Report writing
   - ↳ Inform.
   - ↳ Record-
   - ↳ Demostrate Alertness
   - ↳ Protect
3. Weapons Safety
4. Wearing Firearms.
5. Supervisor
   - Understand ↳ Trends | events | legal | Practices
   - Make ↳ Stress free | clean environment
   - Ensure ↳ right Actions.
   - ↳ open Communication (I|P)
   - Leadership ↳ Appreciate staff (role.

BANK Fraud

↳ It is an illegal activity.

↳ False Info to obtain (money, Assets, property, Financial).

↳ Ex:- Cheque Fraud / Credit card Fraud.

↳ It is an Criminal offence | Imprisonment.

Types of Bank Fraud

① Cheque Fraud

↳ Forging cheque by false sign

↳ Stolen or counterfeiting cheque.

(2) Credit Card Fraud

↳ use someone credit card for unauthorized purchase.

(3) Mortgage Fraud

↳ False info for application in order to obtain loan.

(4) Identity Theft

↳ steal someone personal info.

↳ Eg:- social security Number.
Bank A/C.

(5) Phishing

↳ Email or Text message

↳ Trick people perception with malicious code to gain info.

(6) Money Laundering

↳ convert illegal source money to legal.

⑦ Cyber Fraud

↳ Hacking Bank System to Access A/c Info.

⑧ ATM Skimming

↳ Attach external scanning device to capture the card Information.

↳ Track the ATM Keyboard

↳ Scan card insert slot.

ATM CARD OR SMART CARD

↳ Chip card standard

↳ EMV

- EMV → Visa
- EMV → Europay
- EMV → Master card

Smart Payment System

- Chip and Pin
- Chip and Signature

It follow
↳ chip CARD Standard
↳ ISO/IEC 7816

PIN CONFIGURATION

PIN	NAME	DESCRIPTION
1.	Vcc	+5V or 3.3V DC
2.	Reset	card Reset (optional)
3-	CLOCK	CARD clock
4.	Application specific	AC
5.	GND	Ground
6.	VPP	+21V DC (Programming or NC)
7.	I/O	In/out (Data)
8.	AS	Application specific

→ Structured Card Query language (SCQL)

IDENTITY THEFT

↳ Attack uses personal Info of Victim for malicious Activity.

↳ Info such as (name, social security, DOB)

To Obtain ↳ Credit card, loans, A/c, Access to money or goods.

It consist of three forms (Primary)

- Financial → (Credit card / tax and mail fraud, passing bad cheque)
- Criminal → commit crimes in other person names.

↳ Financial crimes with use of Credit card.

↳ Terrorism.

- **Medical**
  - ↳ Pay the bill for someone else person.

Data behind the Identity Theft (IT)

- ↳ FTC identify that → IT is fast growing crime.
- ↳ 8.4 M peoples in America victims of IT in 2007.
- ↳ Total cost of this crime is about $49.3 billion.
- ↳ Direct cost to consumers is $5 Billion.

Dumpster Diving

Hard copy
- ↳ Garbage scan
- ↳ cheque, ATM slips
- ↳ E-bills, Bank statements

Digital copy
- ↳ Recycle Bin.
- ↳ Trash (Mail).
- ↳ like/favourites.

Vulnerable Personal Information

- Social Security Number (SSN)
- Date of Birth (DOB)
- Mother's / Maiden name.
- Personal Identification Number
- Passwords
- Security Questions.
- Driver License Number.

Vulnerable Information COMES IN Mail

- Telephone Bills or other utility bills.
- Drivers license renewal.
- Monthly credit card statements.
- Bank statements.

What You Throw AWAY CAN HURT YOU

- Pre-approved credit card Application

↳ Credit card Receipts.
↳ Financial statement.
↳ Other Paperwork.

Prevent Identity Theft

when you browse on ↳ web / shop online / login and out secure websites.

share info ↳ social media, banking, online shopping, email, blogs.

Prevent ↳ ① Encryption.
② Authentications.

Finding Your Allies

↳ Federal Trade Commission (FTC)

↳ Social Security Administration (SSA)

↳ Law Enforcement Agencies.

↳ Federal Bureau.

↳ CERT Response Team.