DOMAIN 2

5. PROTECTING SECURITY OF ASSETS

1 Identify → 2 classify → 3 implement security control

Data classification + Asset classification

Security Controls for Data + Asset

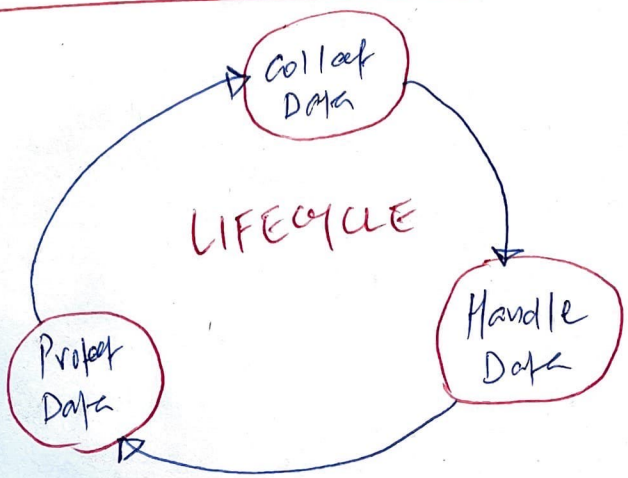
What to Protect?

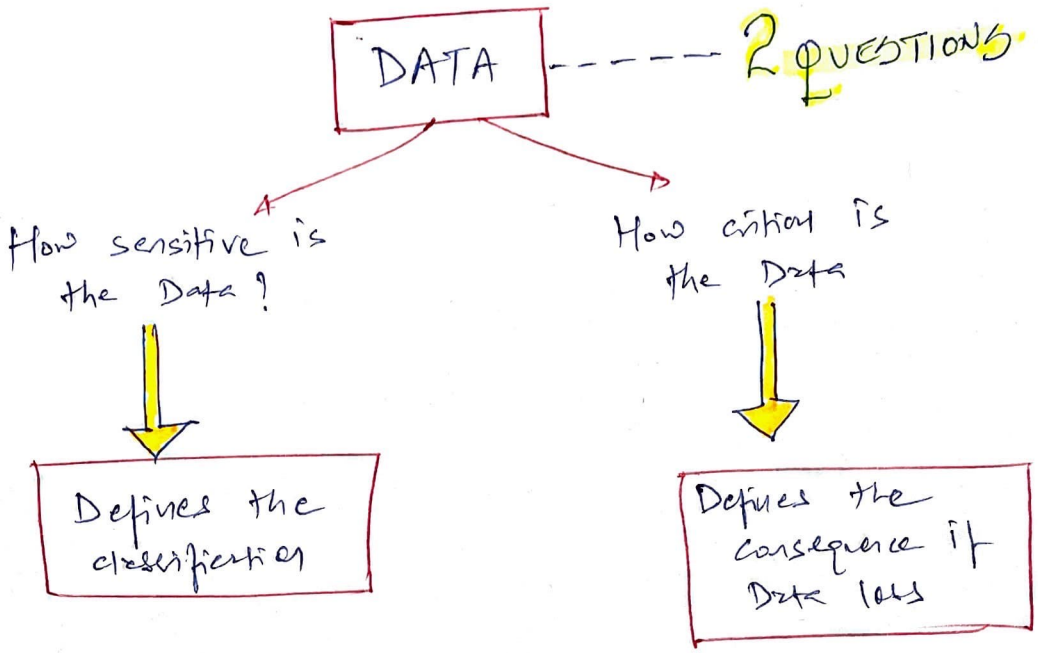
Assets that hold data

Data

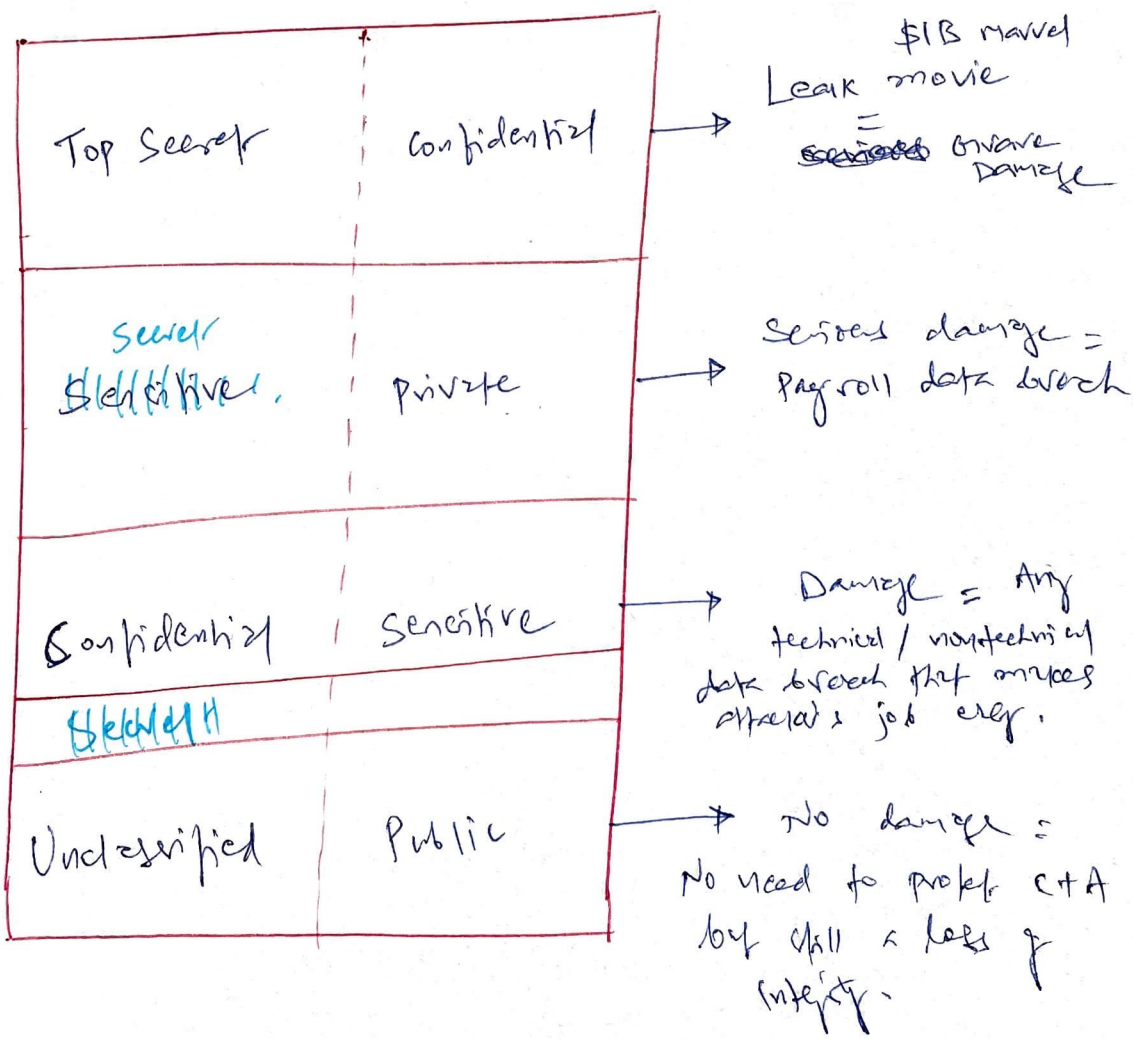
- PII ..... NIST SP 800-122
- Public Health Info. (PHI)
- Proprietary Data
  - Financial
  - Educational
  - Company / Internal process.
  - S/W code
  - IPs

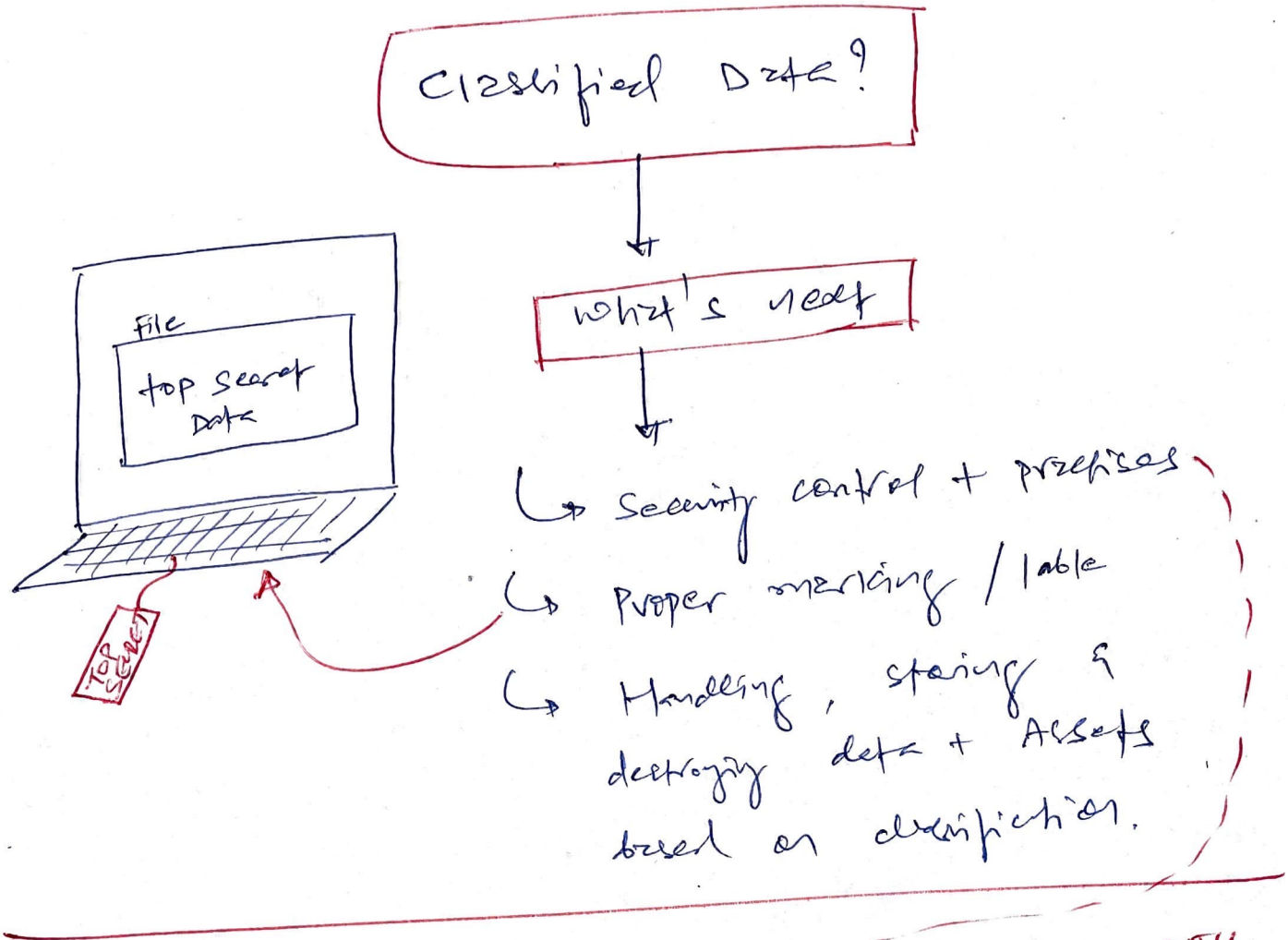
Copyright + Patents are not enough for protection



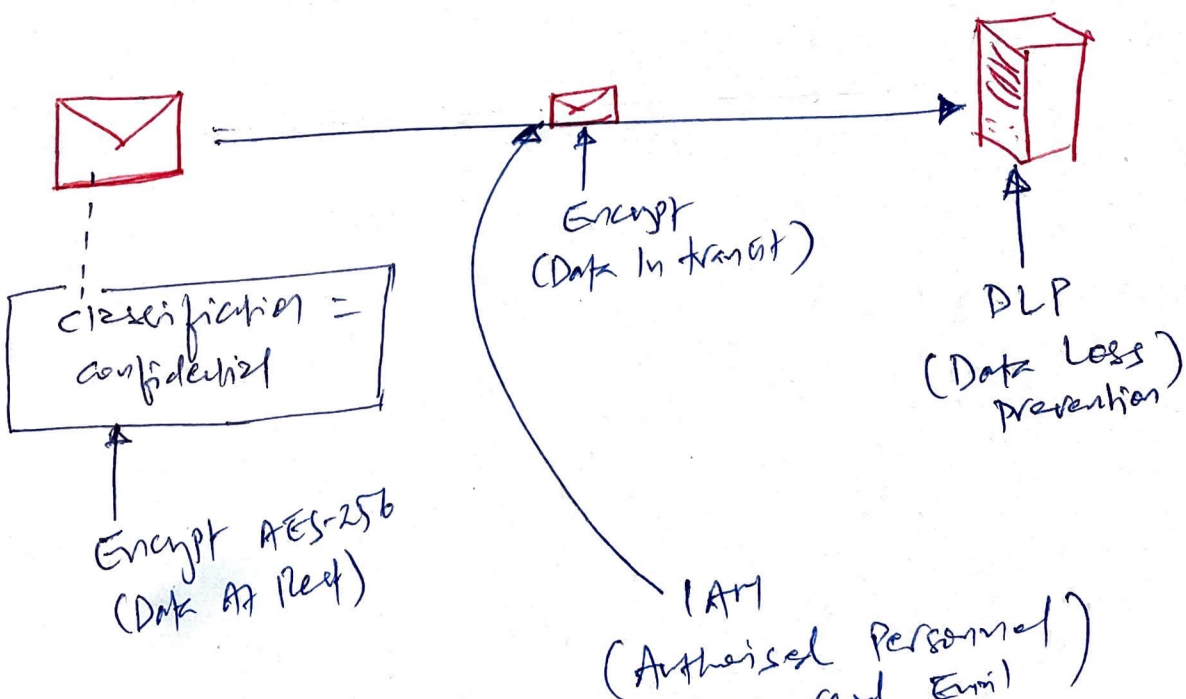


US CAN STOP TERRORISM

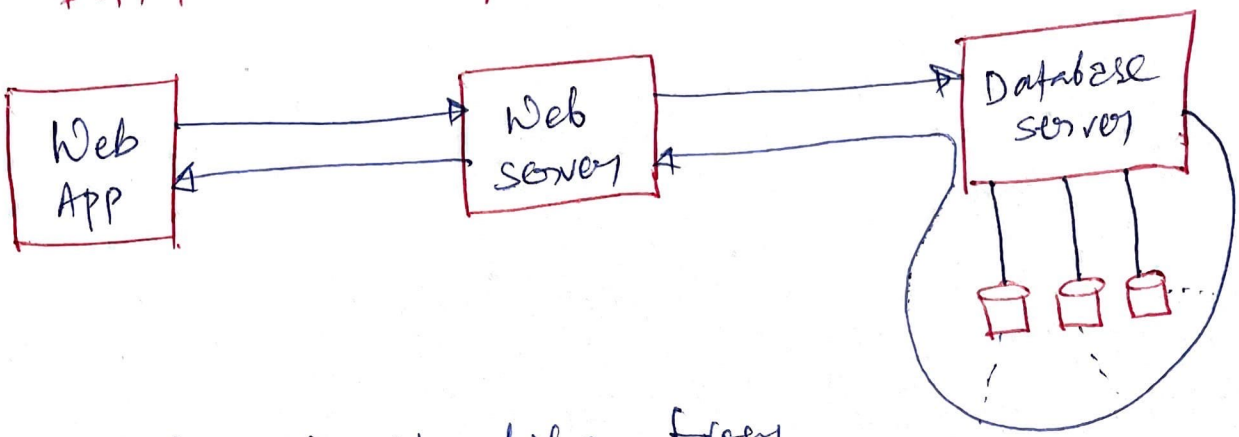




SECURE EMAIL EXAMPLE WITH SECURITY CONTROLS / MEASURES



DATA STATES W/ EXAMPLE

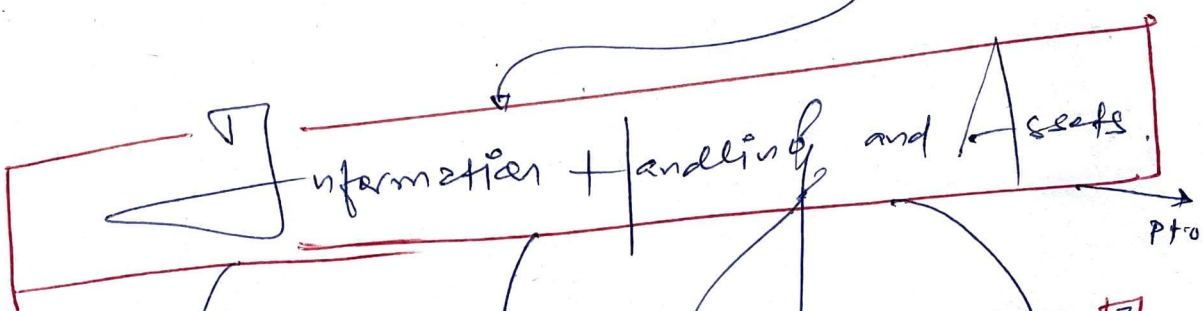


1. Web App request data from web server
2. Web server request data from Database server
3. DB server retrieves encrypted data from Database, convert to (decrypt) format so web App can understand.
   → Data At Rest (AES 256)
4. DB server again encrypt the data & send to web server
   → Data In Transit (TLS 1.2)
5. Web Server decrypt the data & send it to web App. It stores some temp data buffer while authorizing transaction & purge / delete data (from memory) when ~~web App~~ no longer requires.
   → Data In Use (TLS 1.2)

REGARDLESS OF SECURITY CONTROLS

DATA BREACH happens --

To prevent data breach, we need to manage sensitive data



1 Marking
- Physical
- Electronic / Digital
  - Desktop Background
  - Watermarks

Useful for DLP

- Don't downgrade classification instead destroy it.

2 Handling
- Secure transportation of media throughout the lifecycle

Sensitive Data

Backup

Secure both

TD Bank paid $850K for losing 2 Backup Tapes.

3 Storing Sensitive Data
- Encryption
  - Hashicorp secure vault
- Physical control
  - Ac
  - Locked door

$ of Sensitive Data

$ of media holding sensitive Data

4

Destroying Sensitive Data

- High classified Data = complete Destruction
- lower classified Data = overwrite.

It's not just about destroying data, it's how we destroy it. Method matters.

5

Eliminating Data Remanence

Remance

Ex girlfriend's memory trace

Residue: Traces of Data even after deleting it.

~~destroying data methods~~

Erasing
- Not secure

Purging
- clearing process multiple times
- Not ideal for Top Secret data

clearing / overwriting

Phase 1 1010

Phase 2 0101

Phase 3 1101 (replace random digits.)

Degaussing
- works for magnetic types + harddisks
- Not for CD/DVD/SSD.

Encrypted

Destruction

Physical destruction = most secure

Burning (BAD = disposing body.)

ASSET / MEDIA

× → Decrassify + Purge
= $$$$

→ Destroy & buy new media
= less $$$

Data Retention — P.t.o for bigger picture

- What to retain?
- For how long!
- Where it will be retained!

AUDIT LOGS

Retention Period Expires = Destroy the data

--- Boeing paid $92.5 mil for 14,000 Email decrease types.

How can we protect Data?

!- - - more in Domain 3

Data Protection Methods

- Symmetric encryption
  - AES
  - 3DES
  - Blowfish
- Transport encryption (TLS 1.2)
  - Remote VPN
  - IPSec
  - SFTP, SCP

Ownership

who owns the DATA?

who owns the asset?

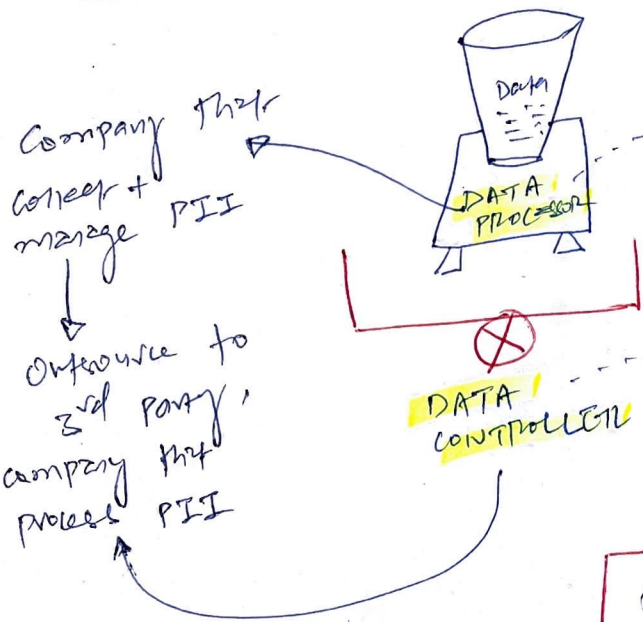
1 DATA OWNERS ---- NIST SP 800-18

same person

2 ASSET OWNERS ---- → Data + Asset are classified + labeled

→ Appropriate security controls are implemented

3 Business Mission owners ---- own business process



Company that collect + manage PII

system to process data

Outsource to 3rd party, company that process PII

Person/ entity that manage data processing

4 Data Processors

European Commission + US Government / Department of Commerce ⟹ SAFE HARBOR PROGRAM

7 Privacy Shield Principles

---→ organization can self-certify using these principles.

↳ (1) Notice :- From organization To customers on
- why info they collect
- why they collect

↳ (2) Choice :- To opt-out / unsubscribe kind of.

↳ (3) Accountability for onward transfer :-

organization = comply (1) Notice & (2) Choice

↓

Forward / transfer info to 3rd party

↳ (4) Security :- of Personal Data

↳ (5) Data Integrity & Purpose Limitation :- only collect info as what's needed

↳ (6) Access : Individual to correct, amend, delete their PII

↳ (7) Recourse, Enforcement & Liability :- Mechanism to handle individuals complaints.

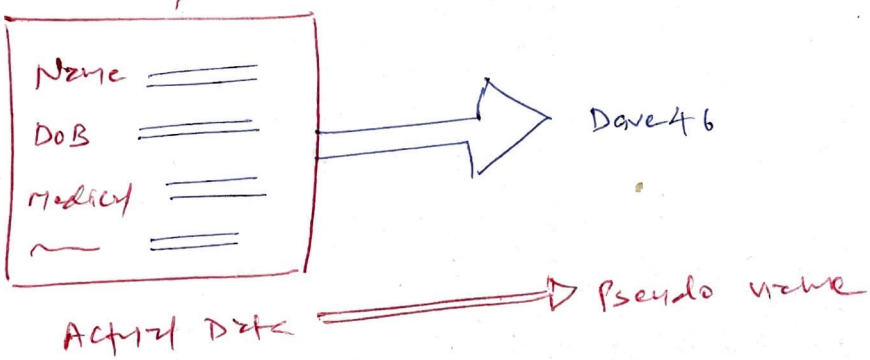
5

Pseudonymization ---- similar to Tokenization

--- GDPR context = Replacing data with Artificial Identifiers.

Sensitive Information Protection

- Encryption
- Pseudonymization.



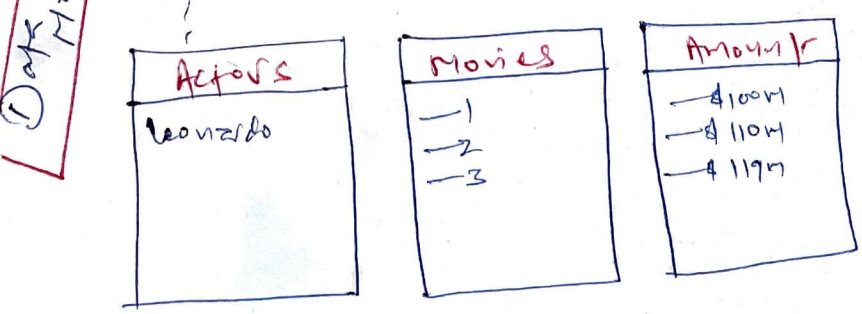
6

Anonymization ---- Removing all relevant data so it's impossible to identify the original data subject/ Person.

BUT, DATA INFERENCE TECHNIQUE can identify individual even if Personal data is removed.

Method

Data Mining



Even if Leo is anonymized, we can still find how much he paid from his movies.

Data Masking vs Pseudonymization / Tokenisation

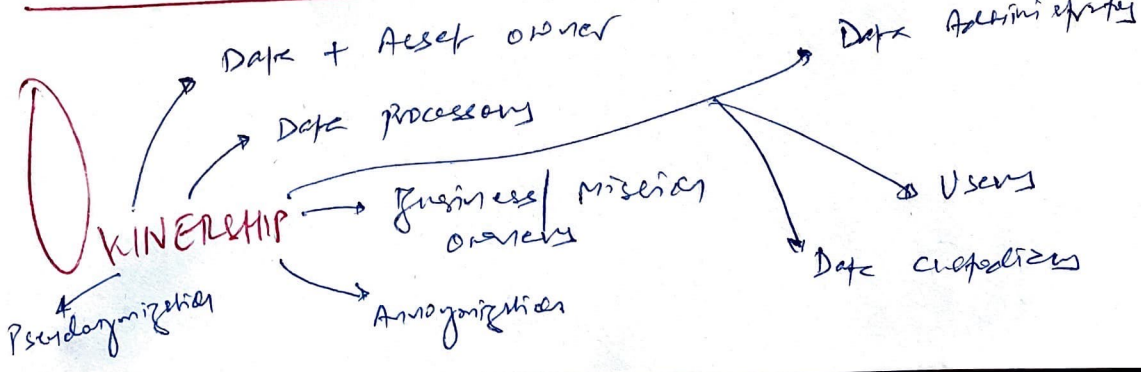
→ once masked, it cannot return to original state.

7 DATA Administrator ----→ Assign permissions based on RBAC / least privilege

8 DATA Custodians ----→ Data owner delegate day to day task to custodians.

- Maintains integrity and security of data
- Data is backed up.
- Data logs maintenance for Audits.

9 Users ----→ Have access to data they only need



To Protect PRIVACY

consider

Security Baseline

↳ NIST 800-53

↳ CIS

Security standards

↳ ISO 27001

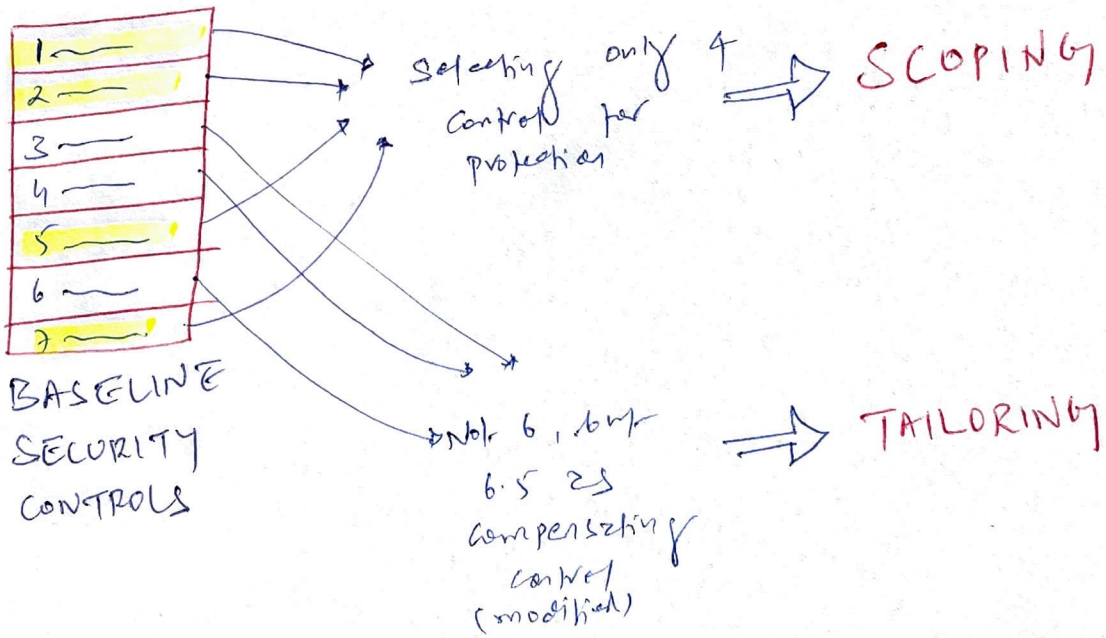
↳ PCI DSS

↳ MAS

↳ GDPR

software images

ch: 16



⭐ Inventories

① Tracking Hardware

Problem : Pirated hardware / stolen or tampered hardware

Solutions: ISO 28000 : 2007
- secure supply chain
- Trusted source
- Trusted transportation network
- effective inspection process

② Tracking Software

Problems:
- distribution of unlicensed s/w in company
- unlicensed s/w without patch = Hole in security
- Pirated software with backdoor entry = trojan

Solutions

solution of software tracking problem = MULTIFACETED

- Application whitelisting
- Using Gold Mastered - standard image for authorised software
- Enforce POLP - Not everybody should install s/w.
- Authorized Scanning - periodic Vul. Scn.
- Device management Software - Unified Endpoint mgmt (UEM)

DATA RETENTION

what data to retain?

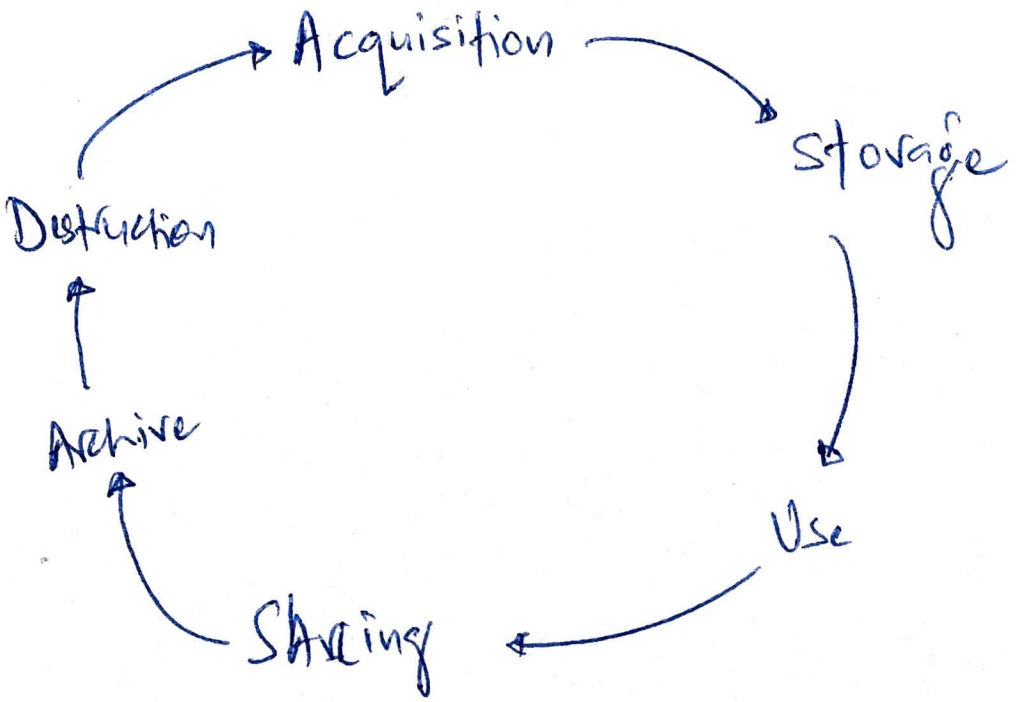
How we Retain Data?

where to retain Data?

To ensure data is available in timely manner, consider four issues:

1. **Taxonomy**
   - Based on various categories
   - 2020, HR, IT, Marketing
2. **classification**
   - Search data based on sensitivity
3. **Normalization**
   - Tagging scheme that make data searchable
4. **Indexing**

INFORMATION / DATA LIFE CYCLE



Note - Introducing Cryptography can add value to data life cycle

- USE = hashing for integrity
- ARCHIVE + DESTROY = Encryption for confidentiality.