# OTHER MONITORING TOOLS

CCTV

Keystroke Monitoring

Record keyboard activity

- video
- H/W
- S/W
  - Keylogger

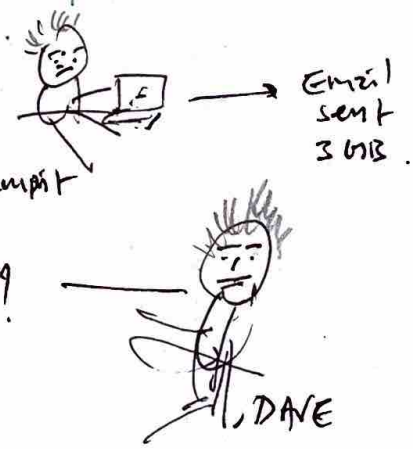
Required to inform employee before monitoring.

Traffic Analysis & Trend Analysis

- Forms of monitoring focused into flow of packets, not the content of the packet.

NETFLOW

- Network flow monitoring




Egress Monitoring

Data leakage

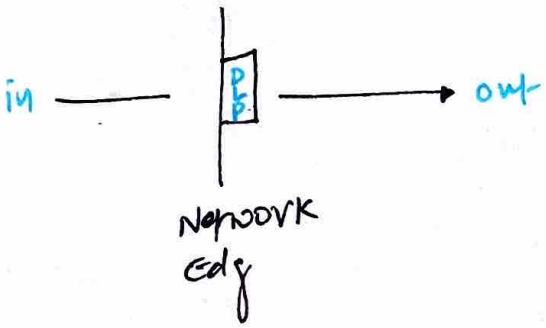
How to prevent Data Exfiltration?

Unauthorised traffic going out

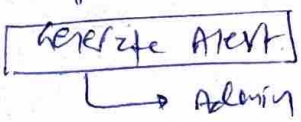
- DLP
- Steganography
- Watermarking

# DLP - DATA LOSS PREVENTION

## Network - Based DLP



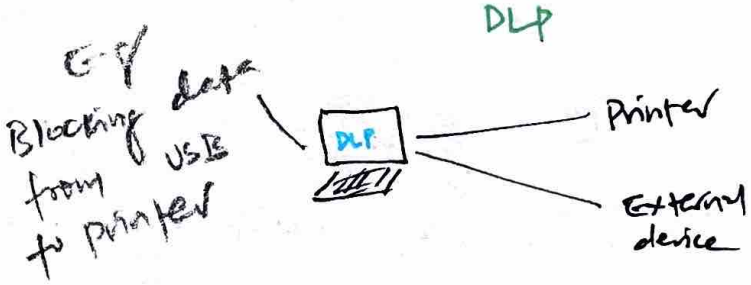

- Scan all traffic going out looking for
  * Keyword * classification * filesize
  * Filetype (MP3) * pattern * watermarking




Need TLS decryption

Note :- DLP doesn't have ability to decrypt data. It scans only unencrypted data.

## Endpoint - Based DLP




- Scans files on system + traffic going out of system

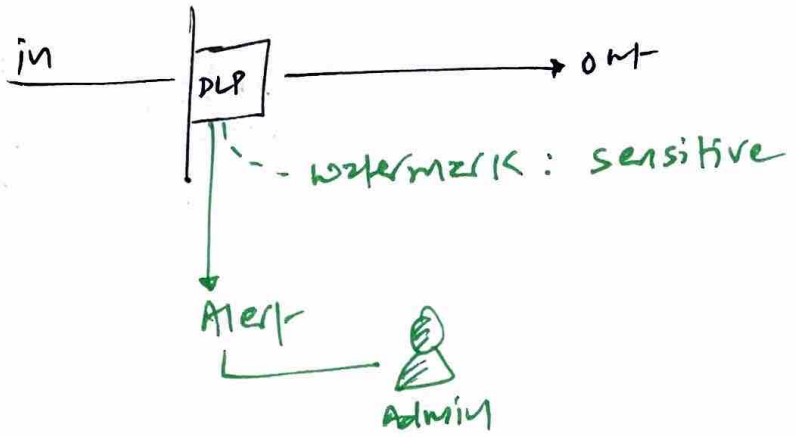
## STEGANOGRAPHY

- Practise of embedding message within a file.

* Using SHA-3, we can compare hash of original & file with hidden message. should come with same hash value.

WATERMARKING + Egress monitoring

→ From DLP perspective
- they can detect "watermark" in unencrypted file.




Studio. Movies use digital watermarking when sending copies to distributors

* Auditing to Assess Effectiveness

↓

Not everybody knows about SECURITY POLICY

we have to

AUDITING → 2 meanings <P.T.O>

AUDITORS

They
- Test & verify Auditing process

Is policy providing security like it's meant to be?

Are people following security policy?

Are there any holes in security solns?

Auditing and Auditing

Use of Audit logs & monitoring tools to track activity.

Inspection (Evaluation) of process / security policies / Guidelines / procedures

* **Inspection Audits**

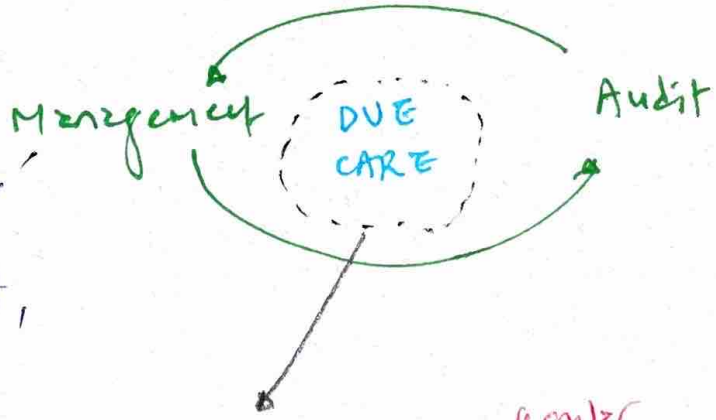
Two important Audits in the context of Access control

Access Review Audits — P.T.O

User Entitlement Audits. — P.T.O

**Audit = time * money**

Frequency of Audit ∝ Risk




that fails Audit, fails due care.

Note - For mgmt, regular security Audits are Due care, if they fail, hold them accountable for any Asset loss. (data)

# Access Review Audits

- Purpose: verify that users don't have excessive privileges and accounts are managed appropriately.
  - Ensures process + policies are in place, working & people are following.

→ Access Review verifies that policy exists and Personnels are following it.

E.g restricted data
- is it classified?
- who has access?
- where & how is data stored?

## User Entitlement Audit

leverages the principle of least privilege

- Reviews which users have excessive privileges
- which security policies are violated related to user entitlement.

while,
User entitlement audit detects whether processes are in place to remove privilege when user no longer need them.

## AUDITS OF PRIVILEGED GROUPS

- Not everybody should be part of Admin AD Group.
- Admin group members use high-privilege accounts when necessary.

Note - Automate membership for privilege accounts in group. So, no one can add or modify manually. ↑ unauthorized user

Dual Admin Accounts

90%.
Admin 1
- Day to day Activities

10%.
Super Admin
- Additional privileges

if Auditing finds = SuperAdmin is used 100%.
⇓
Security policy violation

## * Security Audit & Reviews

Purpose: To ensure that organization has implemented Security controls properly.

From context of Security operation Domain: Security Audit help ensure that management controls (Administrative controls) are in place.

some items to check

- **Patch Mgmt**
  - Vul. scan report helps here
- **Vul. Mgmt**
  - Helps to identify & mitigate vuls.
- **CFG. Mgmt**
  - Ensures original configuration is not modified
- **change Mgmt**
  - Ensures change is implemented as per chg mgmt policy

they are all policies--

* Reporting Audit Results -

What to include in the Report

- scope of audit
- Purpose of Audit
- Discovered results / Revelation from Audit

- - - - How to protect Audit report?

- classification
- Least privilege / RBAC

How to distribute?

- Follow / Refer security policy

* External Auditor

- Issues Interim report: When problem or issue is too important to wait until the final Audit report.
- Holds EXIT CONFERENCE at the end to demonstrate findings, investigations & recommendations.

<Don't Refer this - P.T.O RITUALS>

# INCIDENT MANAGEMENT — Proactive & Reactive process

P.T.O end

Security incident - Declare when IT operation disrupt or we have evidence for breaking security policy

To prevent incidents & detect quickly

Detected incidents dealt properly

## 1 DETECTION

Identification

Implement three types of sensors for detection

Noticing odd Events — Human

SIEM, IPS/IDS — Technical

Alerts from supply chain partners — 3rd party

Analyst receives alert from detection system & verifies the accuracy.

P.T.O

## 2. RESPONSE

Containment → Goal:

To prevent or reduce further damage from incident so we can begin mitigate & Recover.

How?

RESPONSE strategies

Indicate to Attacker that attack has been noticed & countermeasures are in process ---

Target isolation first if possible | containment

If not → Don't power-off system for forensic evidence

change Fw rule or apply ACL to minimize the exposure

Deploy Honeypot as we need more data from Attacker to perform root cause analysis later

# 3. MITIGATION

Eradication

GOAL : We reduced the exposure in step 2 but it's time to properly mitigate the threat by understanding the cause.

Who is the Attacker?

Why is he after?

Exactly, how many systems are affected?

End of this stage : Determine cause & system so we can process toward rebuilding system to good state

# 4. REPORTING — refer to original notes

→ Initial report → Governing Bodies

- Upper mgmt / Stakeholders
- Interim users
- External clients / Partners

# 7. LESSONS LEARNED

# 5. RECOVERY

- Refer to original notes
- Get business-as-usual with change mgmt + Backup / restore

# 6. REMEDIATION

- Perform root cause Analysis & develop security controls to prevent future attack
- GOAL : Now we have security implemented for such types of attacks.

# How do you know – when to call a SECURITY INCIDENT

- IT operation / Business operation disrupts
- Breach of organization's Security policy
- Any intrusion attempt on network or anywhere that targeted company
- Malware infection

from Pituic
Revised incident mgt process – P.T.O

detection / triage

1 – ~~identification~~ / Triage

2 – mitigation & containment & eradication – isolated from n/w

3 – response – Alerting team & responding to incident (SOC Analyst)

4 – Reporting – telling senior

5 – Recovery – chg mgt

6 – Remediation – root cause analysis

7 – lesson learnt – bring diff. department – to improve process

# FROM RITVIK: Incident (Response) Management process.

1. Detection / Triage
   E.g Unauthorised access to system is identified.

Response

2. Mitigation / ~~Containment~~ / Eradication
   E.g All Access to system is revoked & system is disconnected from the network

3. Response (containment) — Mitigation
   SOC
   Gathering team to respond to every

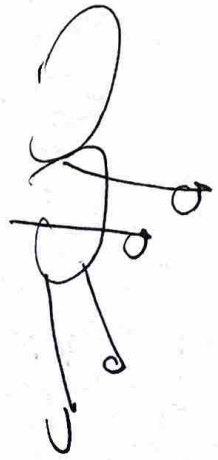
4. Reporting
   - ~~Restoration of effected system~~
   - update senior mgmt.

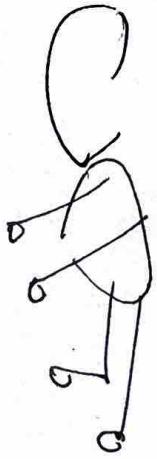
5. Recovery (Aim is to get back to Business)
   - Restoration of effected System
   - change mgmt policy - Business as usual Recovery.

6. Remediation (Then Go to the bottom of the issue)
   - Root cause analysis.
   - implementing controls to prevent future incident

7. Lessons learned.
   - Retrospection: Bring different department to improve process.

# 18. DISASTER RECOVERY PLANNING





Ch: 3

BCP ---- DR ---- This chapter

2 Brothers

↓

Same work

↓

Back to Business

PERSPECTIVE

DR = Technical controls

Prevent disruptions + restore service as quickly as possible

# THE NATURE OF DISASTER

When

I.T = helpless to support mission-critical processes

↓

DRP kicks in

To manage the restoration and recovery procedures.

Plan = Autopilot

↳ less decision making in the event of the disaster

Anything that disrupts normal IT function

Disaster forms

**Natural Disasters**

- Earthquakes
- Floods
- storms
- fires

**Man-made Disasters**

+ Hacking

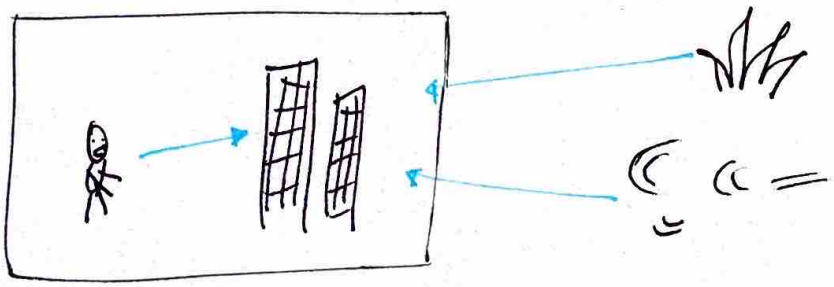
- Fires
- Terrorism
- Bombing / Explosions
- Power Outages
- N/w, Utility & Infrastructure failures
- H/w + S/w failures
- Strikes / Picketing

- Theft / Vandalism

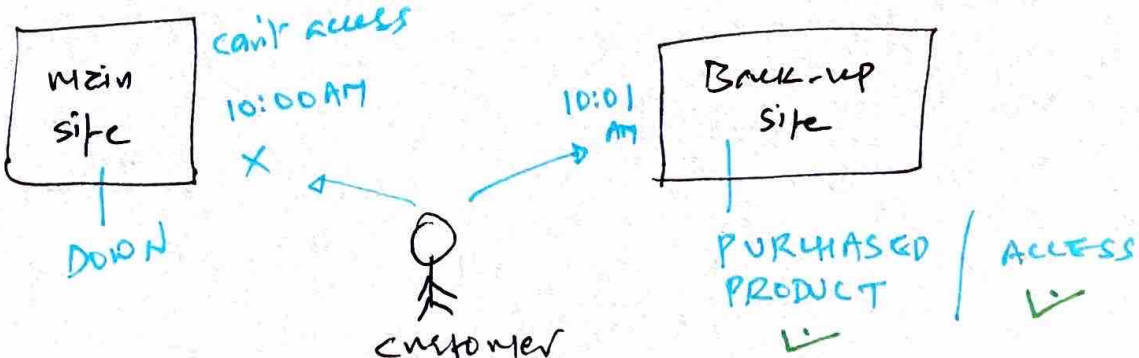
Remember → visuals

(1) Alternate processing sites are far enough away from main site that they are unlikely to be effected by same disaster.


(2) Threats to organisations are internal & external



(3) Disaster strikes without warning. Be prepare to operate backup site as primary in moment's notice.



# UNDERSTAND SYSTEM RESILIENCE AND FAULT TOLERANCE

Goal

To eliminate single-point-of-failure (SPOF)

Thick skin -
Ability of system to suffer a fault but continue to operate. (Not only being available but also allow access to data)

Can run 2K during covid-19 injection

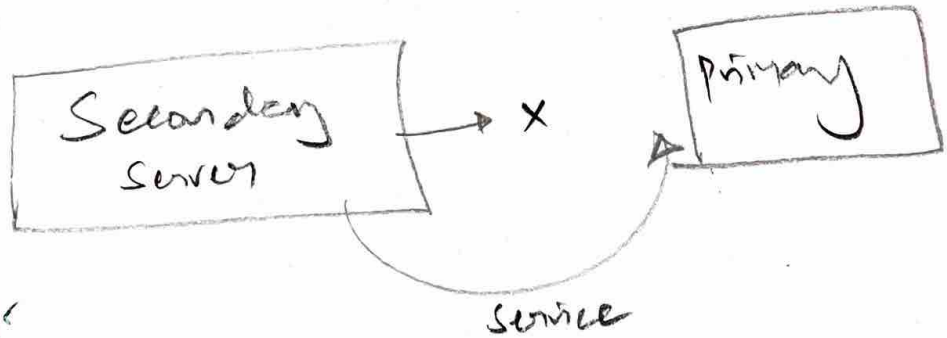
System
Ability to maintain acceptable level of service during an adverse event.

(or)

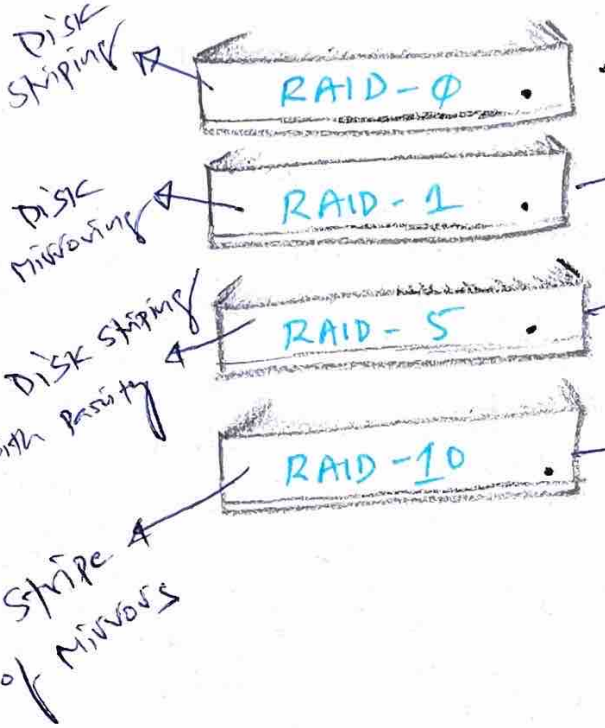
System Ability to return to previous state after an adverse event

Resilient server

Can run at least 10K after covid-19 injection



# * Protecting Hard Drives




RAID 1+0 - at least four drives

↳ Continue to operate if one drive M1, M2 & M3 fails but if two drives in M1 fails - the entire array would fail.

Achieve fault Tol. + system resilience using

RAID Array

H/w RAID

$$$$

Reliable

Supports hot swapping

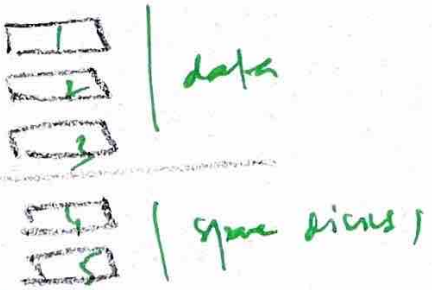
S/w RAID

$$

Need OS

No h/w required

E.g. RAID-5

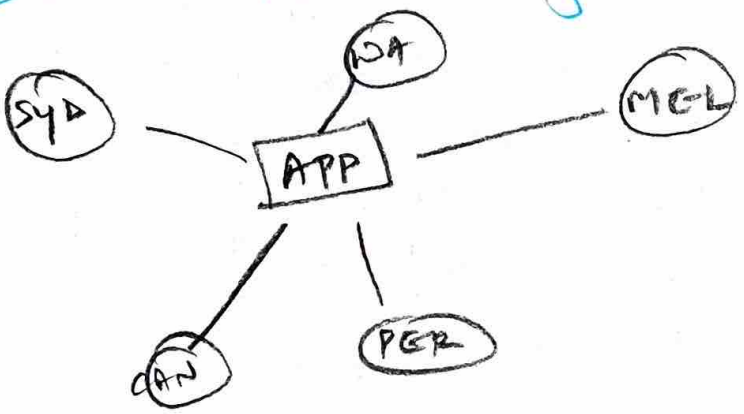


* Protecting Servers

Use load Balancer → To address scalability
                  → Fault Tol.

IaaS providers auto scaling resources on as-needed basis.

Consider DC in different geographical locations




Failover cluster for availability.

consider Automatic Fault Tolerance for servers

↳ Automatic data replication b/w database servers.

* Protecting Power Sources

UPS

- Line-interactive UPS
- for short term

Generator

- For long term
- Needs fuel

* Trusted Recovery

↳ Ensures system is as secure as it was before the failure / crash.

A system can be designed to ~~fail~~ fail either in:

Fail-secure system

default to this state in case of failure

- block all access

Fail-open system

- grant all access

E.g. Firewall, example of Fail-secure with implicit deny philosophy, it will be secure but no availability. If (A) is important, fail firewall with fail-open, it will provide A but not security.

↳ Dilemma P.T.O

Fail-secure

Security but no availability.

Firewall Dilemma

Fail-open

Availability but no security

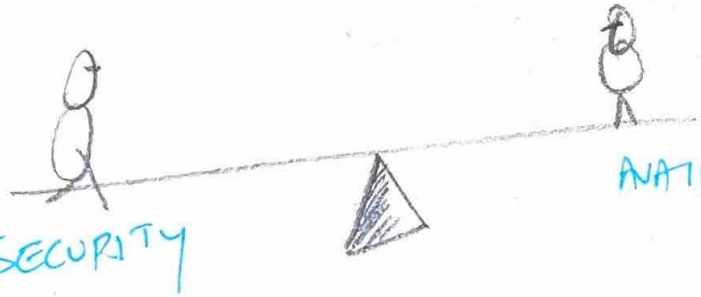
Electrical H/W locks

Fail-secure

- lock if power fails

Fail-safe

- unlock if power fails




---

2 Elements of a trusted Recovery process to implement solution

Failure preparation

- system resilience
- Fault Tolerance
- Backup solution

Process & System Recovery

- Reboot system into normal user A/C & don't allow unauthorised access
- Restore affected files & services

# four types of trusted Recovery:

- Manual Recovery
- Automated Recovery
- Automatic Recovery without Undue Loss
- Functional Recovery

* Quality of Services — depend on some FACTORS

- Bandwidth
- Latency
- Interference
- Jitter
- Packet Loss

# RECOVERY STRATEGY.

* Business Unit & Functional priorities

First — Identify & prioritize critical business functions that you want to restore after disaster & in what order.

BIA (Business Impact Assessment) can help.

BU-1
Recover 50%.

BU-2
Recover 20%.

BU-3
Recover 10%.

Same exercise for 21 business function + process

output should be a checklist of items in priority order

- Risk
- cost
- MTTR (mean time to recover)
- MTO (max. tolerable outage)

BCP Planners assess these values for additional controls

* Crisis management

Results = PANIC Needs → Organised DR Plan

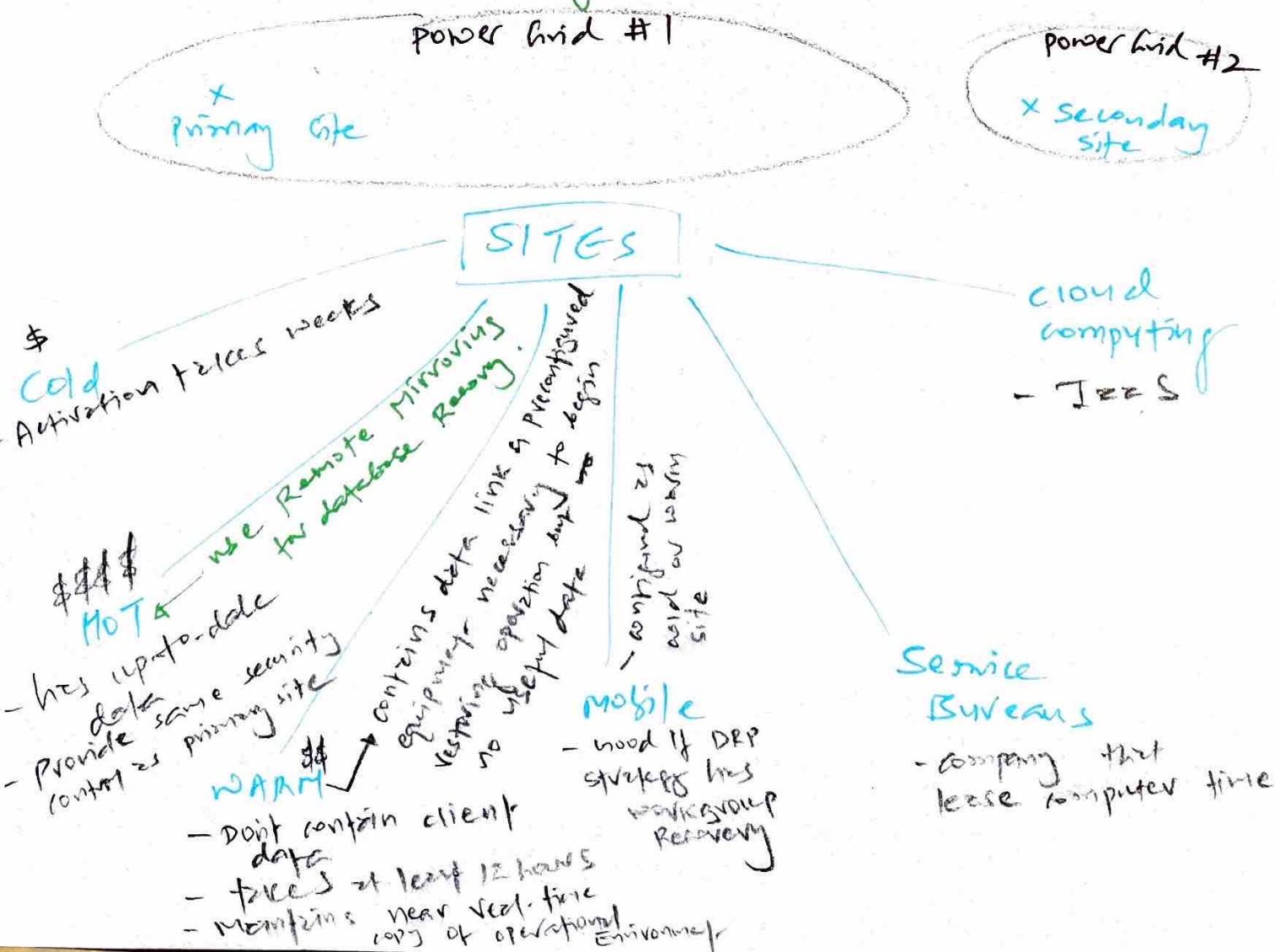
* Emergency communication

Communicate internally & outside the world

* Workgroup Recovery — Mobile site is excellent option

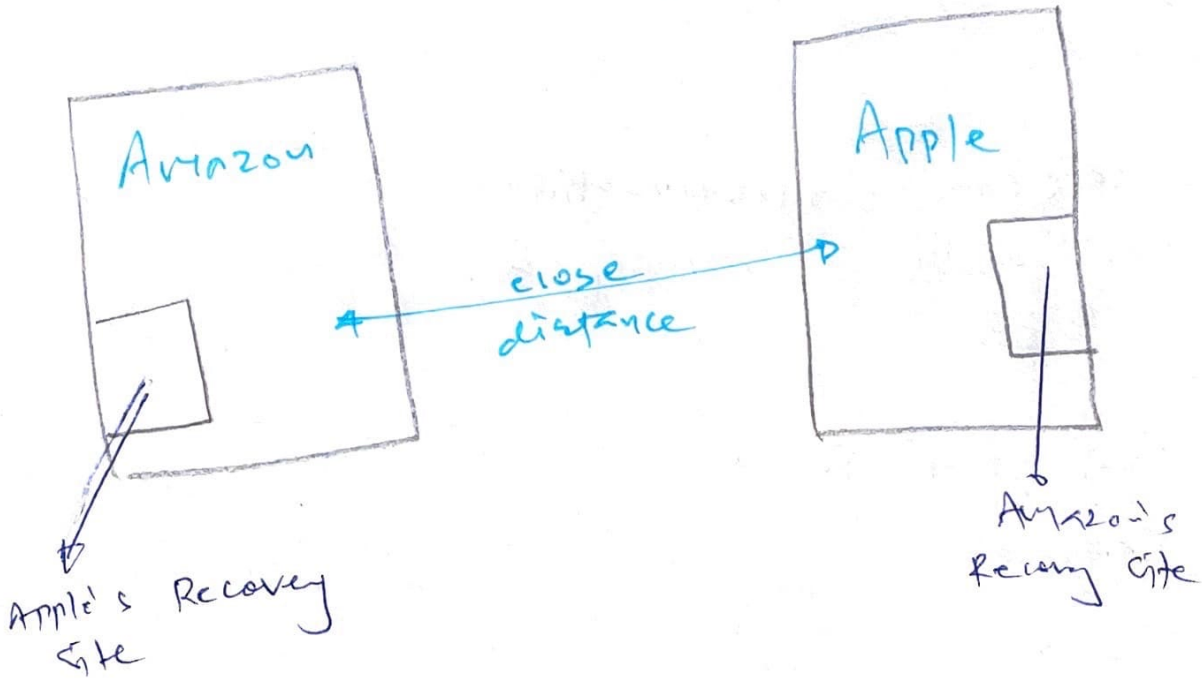
Seperate recovery facilities for different workgroups

* Alternate processing Sites



# * Mutual Assistance Agreements (MAA)

└ Reciprocal Agreement




\+ → cost effective

\- → close proximity may be vulnerable from same threat
- └ Earthquake
- └ power outage

\- → your data into other company! — confidentiality issue

Worst case
└ can't afford Alternate site! → MAA is the saviour

* Database Recovery

↳ crucial part of DRP

3 techniques for offsite database copies

Electronic vaulting
- Backup of Entire database
- Vaulting

- Database backup moved to remote site using Bulk Transfer

Be aware of delay in the disaster event (backup + restore)

- Carefully choose the vendor, consider bandwidth + comms

Periodic Testing with SURPRISE TEST

Ask to restore data on random day

Note - Electronic vault introduces significant data loss. On the event of disaster, you will be able to recover information as of time of last vaulting operation.

Remote Journaling / ~~Mirroring~~ Remote ~~Mirroring~~

- Still bulk transfer but frequent, Also only transaction logs instead of entire DB.

$$$$

Remote Journaling / mirroring → ~~Still bulk transfer but backup frequency (every hour)~~

- Advanced solution = $$$$
- Live database at backup site
- Disaster! Can restore DB in matter of notice
- Ideal for Hot sites