Incident Response

Incident → an event that could be dangerous to the system

event → ~~could~~ ~~be~~ benigh

- Like if a user fails to log in ⇒ event
  1000s of users fail to sign in ⇒ incident

- An event can lead to an incident.

Incident Response ⇒ how you respond to an incident.

IR teams — coordirating ⇓ bunch of IR teams coordination

IR teams models

central ⇓ a company focused on cyper

Distributed ⇓ a large organisation

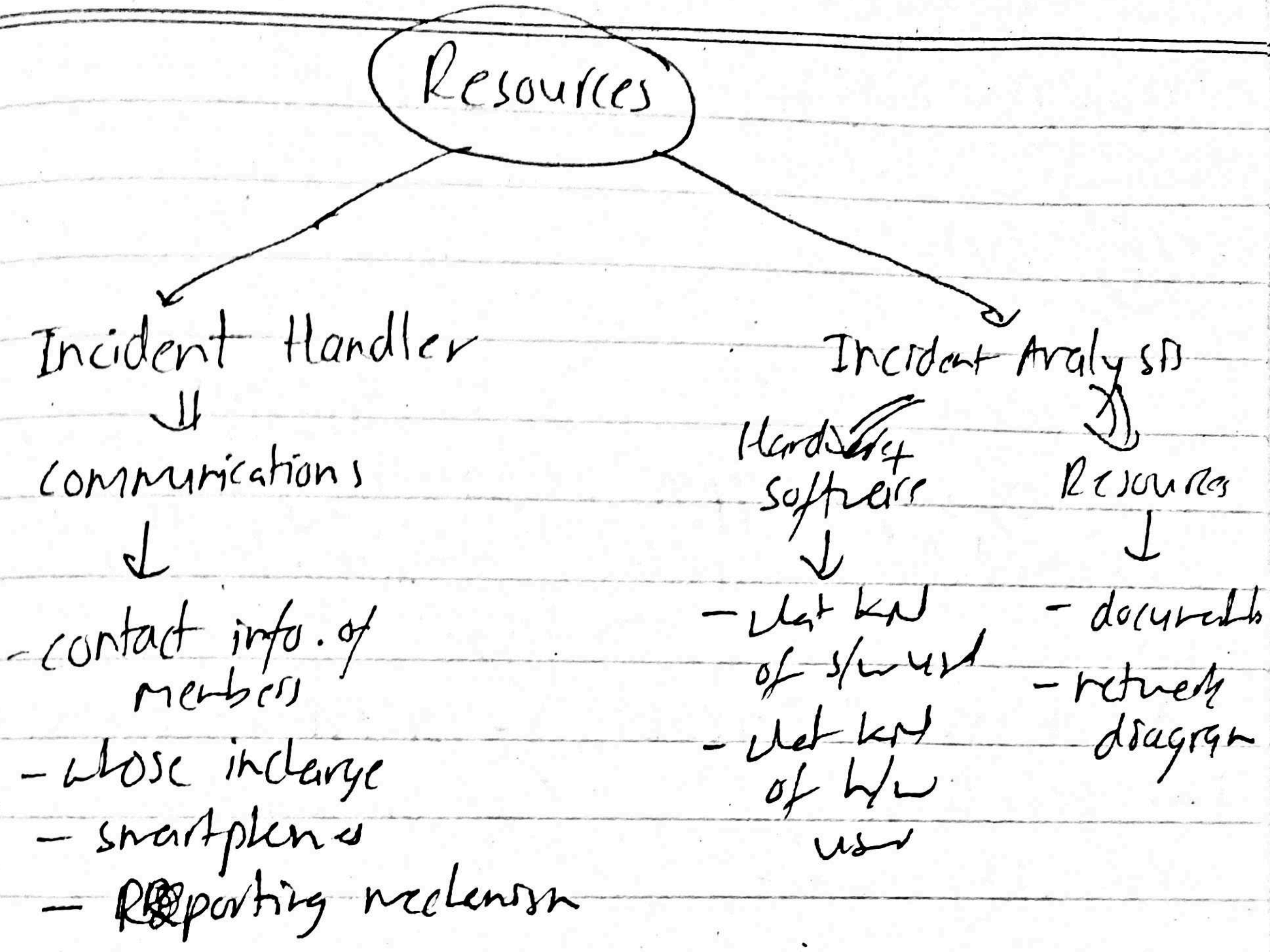
Incident Response Policy

→ the plan of execution

→ policy testing

→ team members + their roles

→ what tools will be used



Resources

Incident Handler

communications

- contact info. of members
- whose incharge
- smartphones
- Reporting mechanism

Incident Analysis

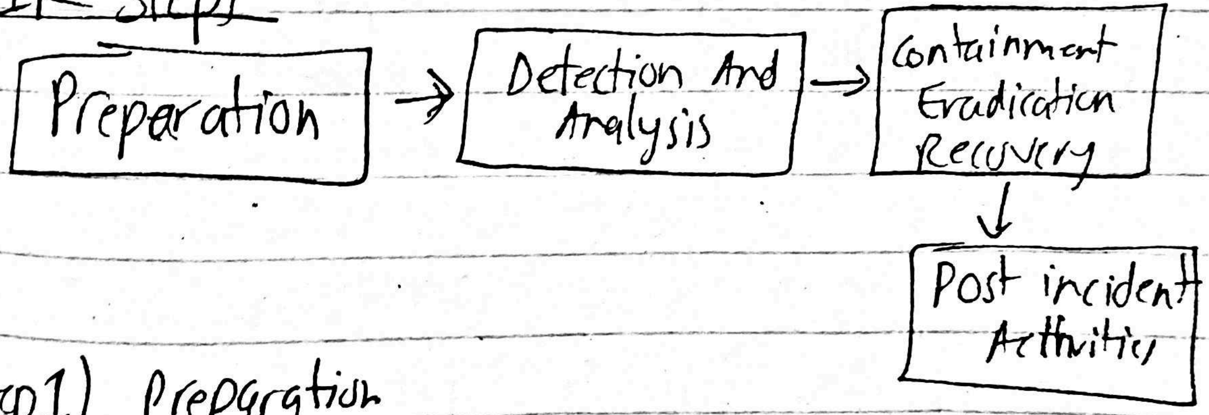
Hardware + Software

- what kind of s/w used
- what kind of h/w used

Resources

- documentation
- network diagram

IR Steps



Preparation → Detection And Analysis → Containment Eradication Recovery → Post incident Activities

Step1) Preparation

- Think 'when' instead of 'if'.

↳ regular risk assessment of system

↳ Users should be made aware of policies and procedures

↳ Configure network perimeters

↳ deploy malware prevention s/w

⇒ Keep no. of incidents low

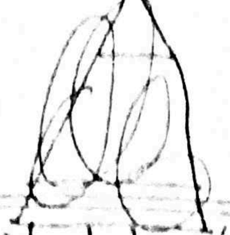
Step 2) Detection and Analysis

A) Detection

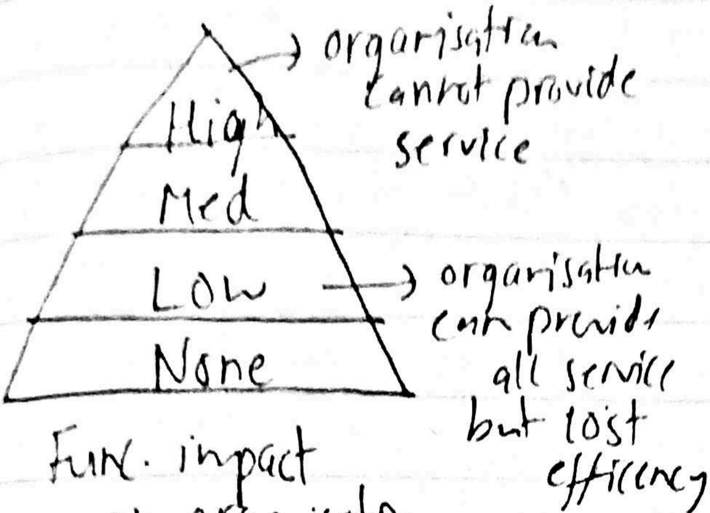
precursor	indicator
something might happen ↳ could be an incident	something happened ↳ an incident
Exa	Exa
- web server log enteries that show usage of vulnerabilty scanner	- antivirus alerts detection of malware
- a threat received from a group that will attack the organisation	- multiple failed logins from remote location

- use monitoring sys. to detect threats
  - ↳ IDS (Intrusion Detection System)
  - ↳ DLP (Data loss prevention) → tools to prevent data loss
  - ↳ SIEM (Security Info. and Event Managment)
    - ↳ analysis events and logs data.

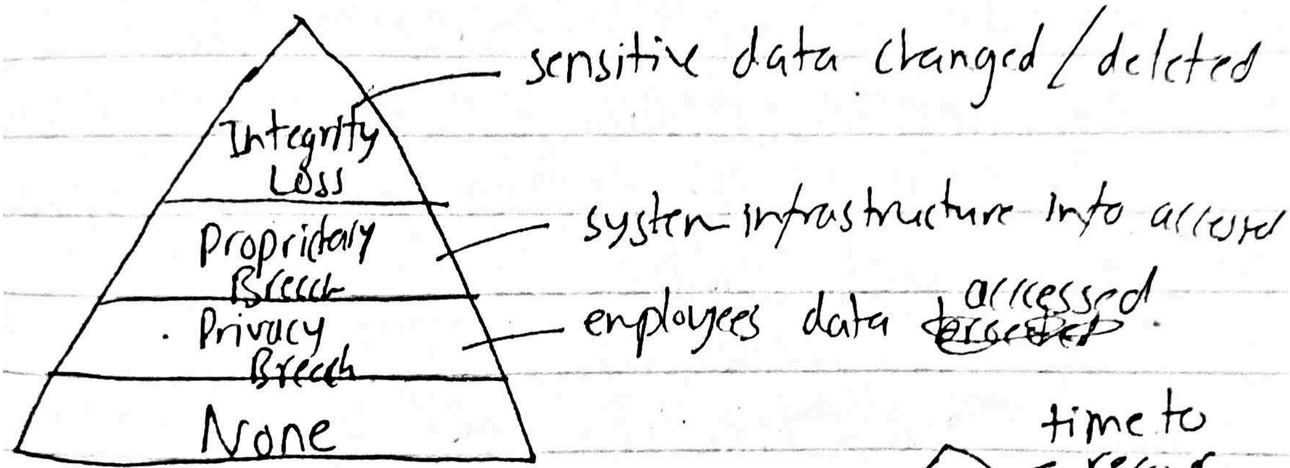
- documentation for incidents
  - status
  - summary of incident
  - action taken by incident handler



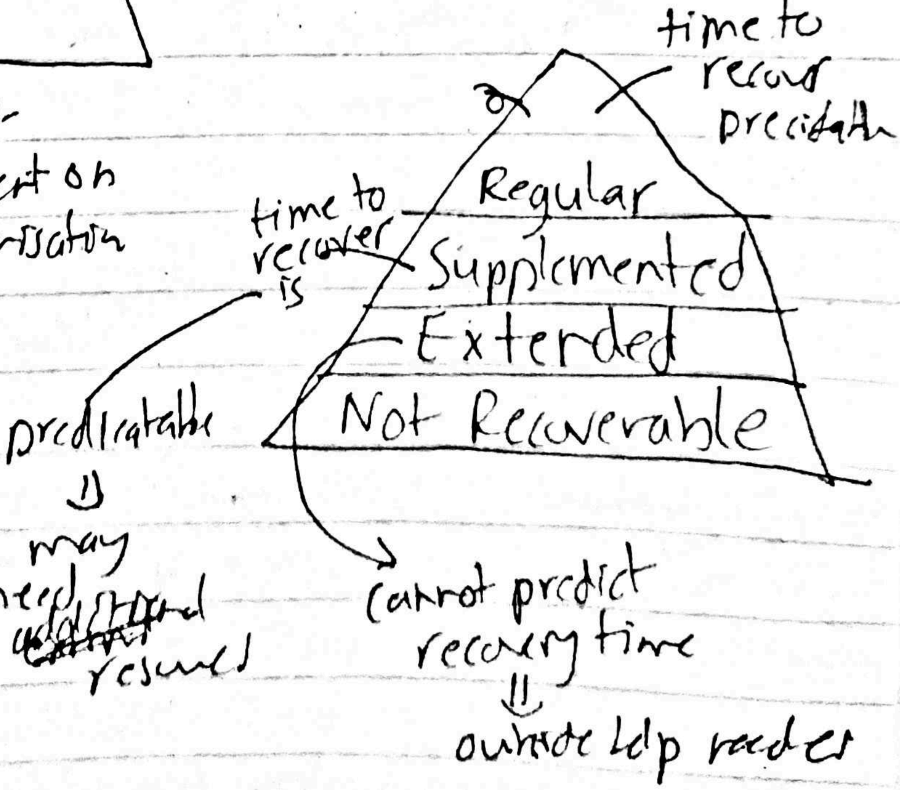
Incident Levels


High
Med
Low
None
organisatn cannot provide service
organisatn can provide all service but lost efficiency

Func. impact on organisatn


Integrity Loss
Propridary Breech
Privacy Breech
None
sensitive data changed / deleted
system infrastructure info accessed
employees data ~~[illegible]~~ accessed.

Info. impact of incident on organisation



Step3) Containment, Eradication and Recovery

→ stop the attack and mitigate further damage,

Containment → ~~stop the threat and mitigate any farthere damage~~ stop the threat. contain it to avoid further damage to resourc

To choose containment ~~stategy~~ strategy things to consider

1) potential damage to resources
2) do we need to preserve evidence
3) time and resource to implement the strategy
4) if threat impacts service how long till service back online
5) effectiveness
6) quick fix or long term solution
   may take months,

Before containment collect evidence
→ forensics

Eradication ~~and Recovery~~
→ eliminate threat + mitigate exploited vulnerabilities

Recovery
- → restore system from clean backup
- → replace comprimised files with clean files
- → install patches, change passwords

- Testing and monitoring to ensure restoration successfully step 4) Post incident activity

→ lesson learned meeting by all parties involved

how well did we do

could it be better

room for equipment

other activity

↳ utilise collected data → what event should be handled faster

this system has flaws

why did this take so long

↳ revisit ~~evidence~~ documentation → IR policy

identify any gap

Incident Response Tools

- Cynet 360
- Google's GRR Rapid Response
- AlienVault
- Cyphon
- TheHive Project