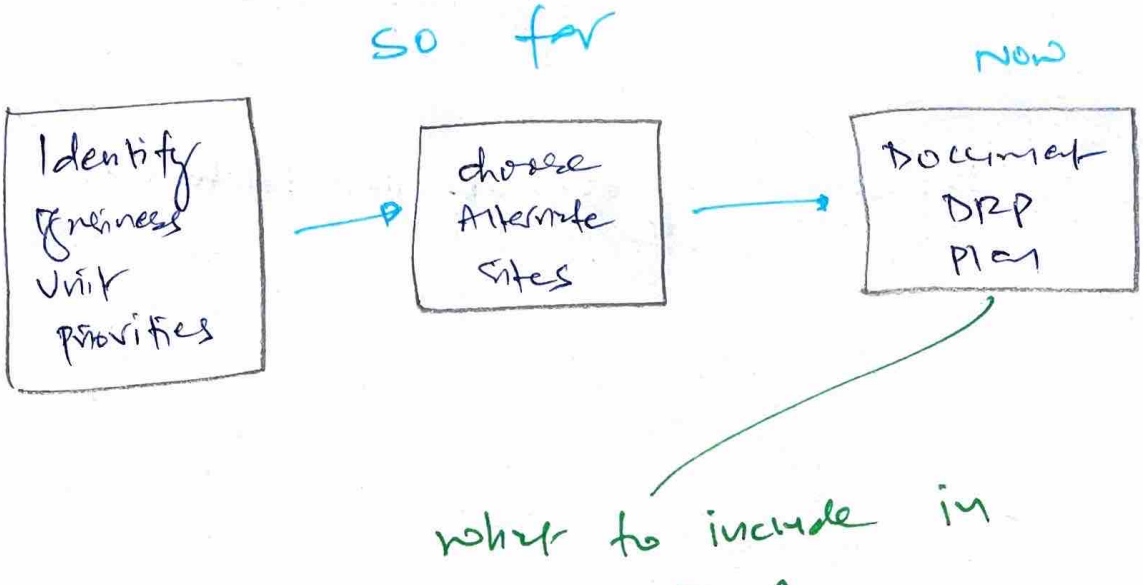
RECOVERY PLAN DEVELOPMENT



- Executive summary - 10,000 ft of DRP plan
- Department specific plan
- Technical guides such as Backup Sq.
- checklist for individuals.
- Full copies of DRP to Recovery team members.
- And below sections

* Emergency Response = checklists

One principle in mind
=
Arrange checklist tasks in order of priority - most important task first

* Personnel and Communications

Key DRP members + Personnels who would perform DRP tasks.

should include Backup contact if primary not available

* Assessment

DRP Team's first task when Arrive on site → CIRCUIT - Assess the situation

* Backups and offsite storage

What's the backup strategy for DRP?

Part of technical guide

BC + DRP's most crucial Element → Backup Strategy.

P.T.O = types of backups

3 Types of Backups:

Full Backups

- stores complete copy of data

Incremental Backups

- stores only those files that have been modified

Faster to backup but it takes more time to restore

Differential Backups

- stores all files that have been modified since time of most recent backup

takes longer to backup than incremental but it's faster to restore

Difference is in time needed to restore the data

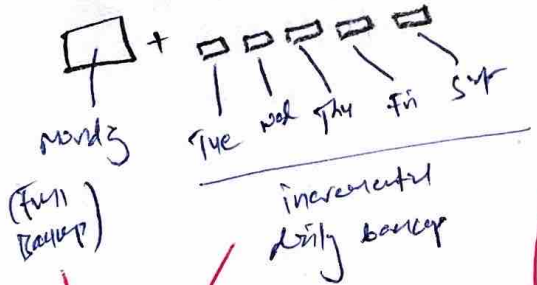
CORE CONCEPT

Common Strategy

- Full backup on weekend & incremental or differential backup on nightly basis

Strategy #1

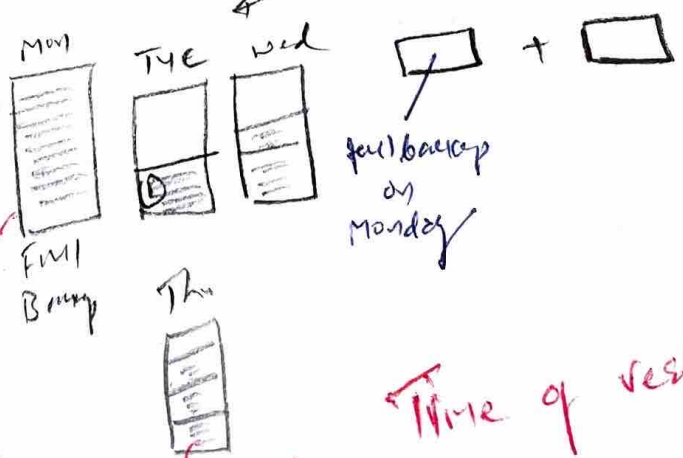
Full + incremental



Need all of them to restore, one if 'Tue' is corrupted!

Strategy #2

Full + Differential



Time of restore! only these two needed

Backup Type Formats

Physical characteristics

- Type of backup media
- old = less reliable

Rotation cycle

- Frequency of backup
- Retention length

Disk-to-disk Backup

↳ D2D backup strategy for DRP

↳ virtual tape libraries (VTL) : uses software to make disk storage appear as tapes to backup s/w.

↳ Consider geographical diversity

Backup Best practise

- Night backup
- Deploy real-time backup → RAID cluster | server mirroring
- Test recovery process

Tape Rotation

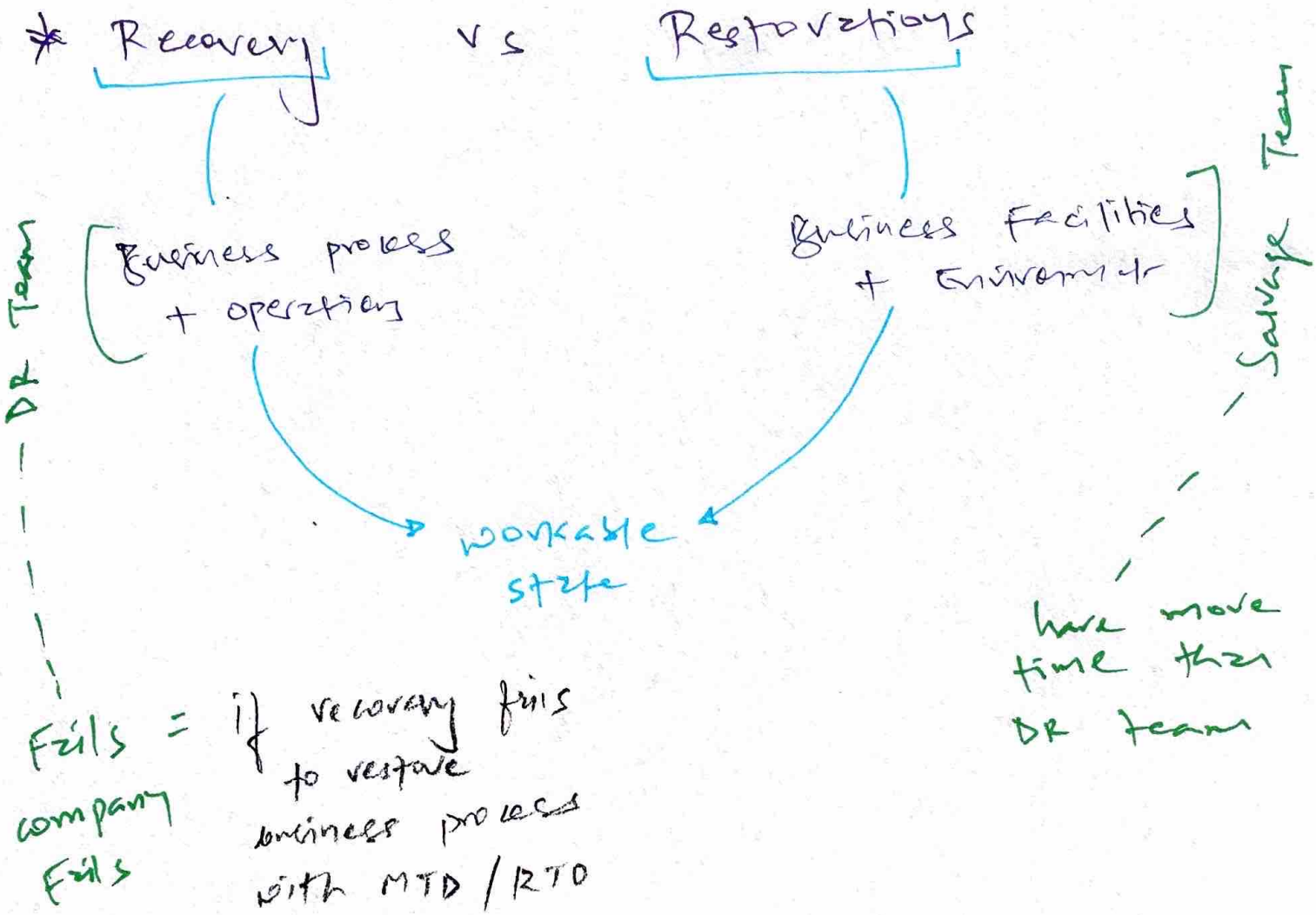
* Software Escrow Arrangements
  - Part of DRP plan

* External Communications
  - Media, Government authorities, vendors, suppliers, customers
  - comms to them = part of DRP.

* Utilities
  DRP to include contact details for Gas, Electricity, water ...

* Logistics & Supplies
  People may live at alternate site for extended period

*
  DRP to provision food, water & supplies for people


* Recovery
vs
Restorations
DR Team
Business process
+ operations
Business Facilities
+ Environment
Salvage Team
workable
state
have more
time than
DR team
Fails = if recovery fails
to restore
business process
with MTD / RTO
company
Fails

TESTING & MAINTANANCE → P.T.O context

TRAINING, AWARENESS & DOCUMENTATION

Read-Through Test
- Send DRP to team member for review

Structural Walk-Through
- Table Top Exercise
- DRP team gather in room for discuss scenario

Simulation Test
- DRP team presented with scenario & asked to develop appropriate response

Parallel Test
- Personnel to go to site alternate site to activate process, pretend that main site is down

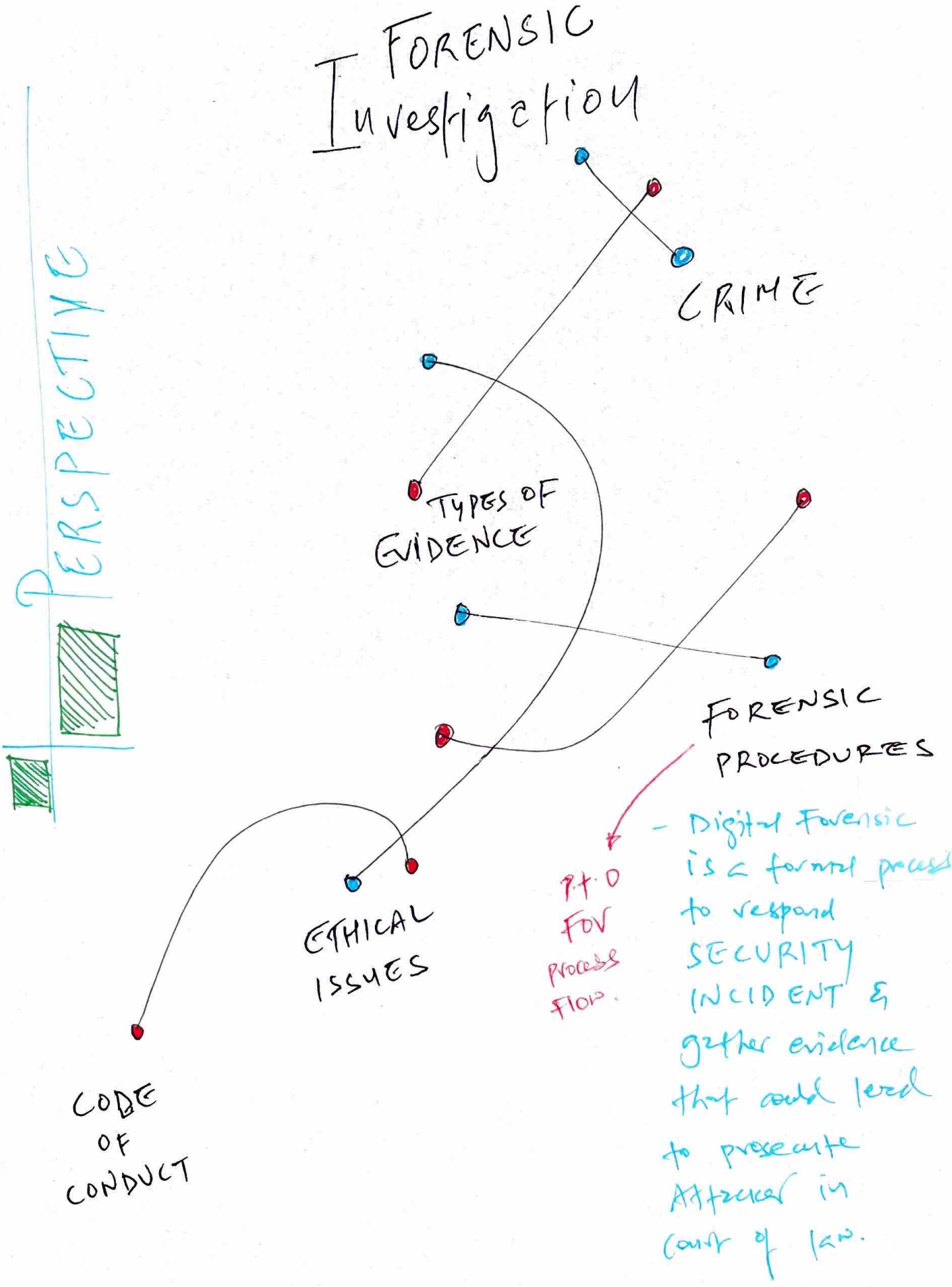
Full-interruption Test
- Actually shut-down primary site & activate DR site
- This is risky
- Most don't like this

Maintenance
- DRP = living document

Any changes in organization must reflect DRP

- DR plan = should refer organization BC plan

19. INVESTIGATIONS AND ETHICS



P.T.O FOR Process Flow.

INVESTIGATIONS

Types

1. Administrative
   - internal investigations
   - To Resolve operational issue
   - Not much evidence required, Performs root cause Analysis
2. Criminal
   - strict evidence collection + Preservation process
   - violation of criminal law
3. Civil
   - Involves internal employee + outside consultants
   - Involves civil court to resolve dispute b/w two parties
   - Not intense evidence collection
4. Regulatory
   - Government agencies
   - PCI DSS ! or pay fine $$$$

eDiscovery facilitates process of electronic info. for disclosure.

Purpose: Gather potential evidence to build the case.

Electronic Discovery (eDiscovery)

- To preserve digital evidence, 9 steps
  - Info. Governance
  - Identification
  - preservation
  - Collection
  - Processing
  - Review
  - Analysis
  - production
  - presentation — present in court + other parties

Evidence

Admissible Evidence has 3 requirements

- Relevant
- material (related to case)
- competent (obtain legally)

3 Types of Evidence

1. **Real Evidence / Object Evidence**

2. **Documentary Evidence**
   - written items such as computer logs
   - Best Evidence Rule
   - Parol Evidence Rule

3. **Testimonial Evidence**
   - Testimony of witness
     - Direct Evidence
     - Expert opinion
     - Hearsay Evidence

if logs are not authenticated, are hearsay Evidence = contraband

P.T.O End

Investigation Process

P.T.O

Evidence Collection & Forensic Procedure

Don't play with original evidence, investigate with copy

Forensic Analysis

P.T.O End

- Media Analysis
- Network Analysis
- Software Analysis
- Hardware/ Embedded Device Analysis

Investigation process — P.t. 0 End for Entire process

* First build Awesome Analyst Team

1. Gathering Evidence (collecting Evidence)
   - is important but how to confiscate is more important

3 Alternatives for evidence gathering

- Person who owns evidence voluntarily surrenders it.
- Get court to issue subpoena / court order
- Last option based on ~~reason~~ probable cause — surgical strike — search warrant

This leads to surrender evidence

ANOTHER STEP — Add in the policy

Add to provide consent to search for evidence for new employees as part of Employment agreement

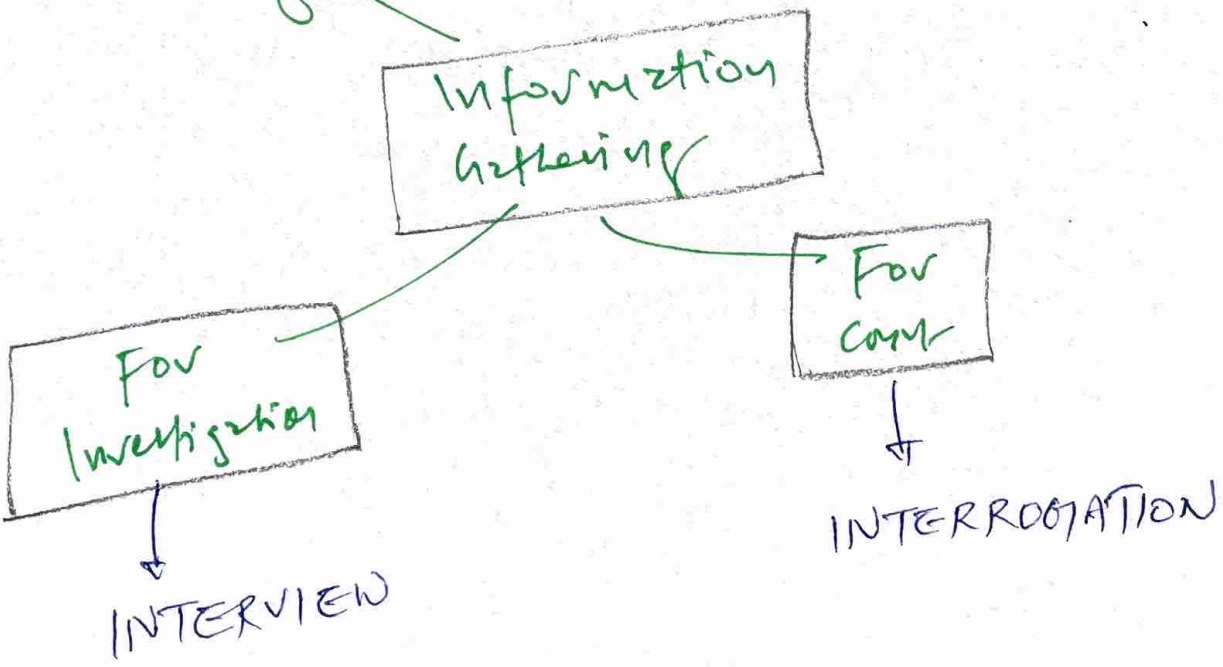
- Calling In Law Enforcement
  - 2 factors company may not call FBI
    - Public Embarrassment
    - Investigation may reveal other wrongdoings

conducting the Investigations

FBI Alternatives + Tips

- Don't investigate an actual compromised system
- Hire Private Investigator
- Don't Hack back to avenge. Might hurt innocent 3rd parties.

Interviewing Individuals



- Always contact attorney before conducting any interviews.

Data Integrity and Retention

- maintain the integrity of the evidences and integrity of the data before you collect from the crime scene

how? p-t-o

↳ Simple Archive Policy : Ensures key evidence is available upon demand no matter how long ago incident was occured.

↳ Protect integrity of log files : (Remote logging + Use of Digital Signatures)

All systems send log records to secure centralised server

↳ Reporting & Documenting Investigations

Start of Investigation

↓

Administrative / internal

— can turn into criminal investigation —

Be prepared

Prepare formal documentation.

Establish relation with legal corporate team + law enforcement agencies

Find single contact to liaise with law enforcement

Easy for all "go-to" updates for one person

Predesignated contact to work with law enforcement

MAJOR CATAGORIES OF COMPUTER CRIME

Understand the attack + attacker

helps → How to protect & Recover

helps → What evidences to look for after the attack

① Military & Intelligence Attacks

Goal: To obtain restricted / secret information

How To protect: → stringent perimeter security
→ Internal controls

Evidence: Usually no evidence to collect as Attackers are pro - Next level

② Business Attacks

Goal: To illegally obtain organization's confidential information

How To protect: Risk mgmt + controls

Corporate / Industrial Espionage

MOVIE NAME

③ Financial Attacks ← Shoplifting
← Burglary

Goal : To obtain money

- $1000 ← Newbie
- $1000000 ← Sophisticated Attacker

④ Terrorist Attacks

Goal: To disrupt normal life & instill fear

JOKER

Future of Attack — physical Attack + computerized Attack (simultaneously)

Prevent: 24x7 monitoring

⑤ Grudge Attacks

Goal: To damage person / organization reputation + loss of information

FIRED EMPLOYEE

Protect: Security policy — disable all access of terminated Employees

↓

Perform Vul. Assessment for "Back Doors"

⑥ Thrill Attacks

How: To have Fun

By SCRIPT KIDDIES: Attackers use other people's programs/scripts to launch the attack.

Most. consequence of Attack: Service interruption (most common)

E.g: Website defacement
Attacker replace legitimate webpage with other one

Rise of Hactivist — Hacker + Activist — political motivation with thrill of hacking

---

FORENSIC DISK CONTROLLER FUNCTIONS

what it is?

- Write blocking
- Intercepts write commands sent to device
- prevent them from modifying data on the device

- It's a hardware write-block device made for the purpose of gaining read-only access to computer harddrive without the risk of damaging the drive's content.

ETHICS

Two code of Ethics

- $(ISC)^2$ code of Ethics
- Ethics and the Internet

(1) Protect society, the common good, necessary public trust, and confidence and infrastructure.
- public safety

(2) Act honorably, honestly, justly, responsibly, and legally.
- Duties to principals (सिद्धान्त, आदर्श, उद्देश्य)

(3) Provide diligent and competent service to principals.
- Duties to Individual

(4) Advance and protect the profession.
- Duties to profession.

Forensic Analysis

Media Analysis

- Identification & extraction of information from storage media.
  - magnetic media (hard drive)
  - optical media
  - memory
- Techniques → Recovery of deleted files from unallocated sectors from physical disk
  - Static Analysis of forensic images of storage media

Network Analysis

- Activity that took place over network during a security incident.
  - IPS
  - Netflow
  - packet capture
  - logs from firewall

E.g. Reviewing logs from web server is network analysis.

Software Analysis

- Forensic look for s/w / Application source code for
  - malicious code
  - Backdoor activity
  - logic bomb
  - or review database file for SQL injection
  - Review privilege Access & other Application Attacks

Hardware / Embedded Device Analysis

- Need experts who has specialized knowledge in
  - memory
  - OS
  - storage

4th Amendment - Prevents law enforcement agencies from searching home/facility without consent or probable cause

1st Amendment - Protection related to freedom of speech

5th Amendment - Ensures no person will require to serve as witness against themselves.

15th Amendment - Protects the voting rights of citizens.

Testimonial Evidence

Direct Evidence
- when witness testify about their direct observations

Expert opinion
- Allows individuals to offer their opinions based on facts + personal expert knowledge

Hearsay Evidence
- Testimonial evidence should not be hearsay
- Someone told me blah-blah outside the court
- E.g. logs that are not generated by server is hearsay evidence

Real Evidence → tangible items

Documentary Evidence → consists of written records

ISO/IEC 27037 Guidelines for Digital Evidence

Digital Forensic Process

4 steps

1. **Identification** of Evidence — Maintaining integrity is critical before collecting evidence & after that we present in ~~court~~ court

2. ~~C~~ **collection** of Evidence
   - labling evidence with date, time, location
   - chain of custody (chain of evidence) is crucial

3. **Acquisition** of Evidence
   - creating forensic image of digital data for examination (primary image & working image)
     - primary image → stored in library
     - working image → For Analysis
   - Acquisition also means to collect evidence from volatile sources such as RAM, cache, temp file system & special disk sectors.

~~3~~ Analysis of Evidence - - - - - - - - -

4. **Preservation** — Already: chain of custody & use of hash to maintain integrity
   - Ensuring minimal authorised personnel
   - has access to digital evidence.
     - ↳ implement MoM control

The Forensic Investigation Process.

1. Identification of Evidence
   - Identify your assets that were affected.

2. Preservation of Evidence
   - chain of custody from time of seize to time when present in court
   - To maintain the integrity throughout forensic lifecycle

3. Collection - Tracing control legally
   - Gathering Evidence
     - volunteer
     - court issue subpoena
     - search warrant
     - corporate policy
   - Admissible evidence
     - Relevant
     - Material
     - Competent

4. Examination - Time consuming → Tools & forensic
   - Document findings
   - create forensic image (should be part of preservation)
     - primary image
     - working image → Examine with this copy

5. Analysis — find the root cause
   - Analysis types
     - Media
     - Network
     - Software
     - Hardware
   - what root cause does the evidence point to?

6. Presentation (Reporting)
   - Present evidence in court, may need Expert to testify
   - Evidence Types
     - ~~Direct~~ Real
     - Documentary
     - Testimonial
       - Direct
       - Expert opinion
       - Hearsay

7. Decision
   - Are they guilty or not?