DATACENTER

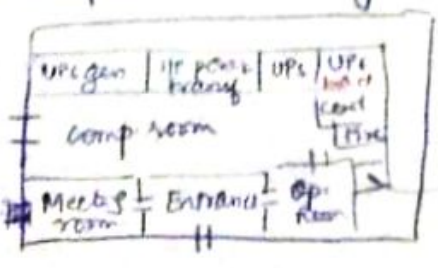
Most IT infra H/W, except end user devices is hosted in datacenter.
Datacenter provides power supply, cooling & fire prevention, equipment racks

Datacenter Building Blocks

* Datacenter Categories
  - → Sub equipment room / patch closet : contain patch panels for connections to wall outlets in offices, & small eq like N/W switches
  - → main equipment room: small datacenter in office
  - → Org. owned datacenter: main central IT eq
  - → Multi-tenant datacenter: used by service providers for multiple organizations

* Datacenter Location
  - → Environment :
    - * Enough space to expand the datacenter
    - * Floods / Hurricane / Earthquake / Fireworks storage / waste dump / chemical plant / climate / (should be low ambient with low fluctuations)
    - * Crime Rate / Vandalism / Near Airport (crashes)
    - * Easily reached in emergencies? Close to maint' staff
  - → Utilities :
    - * 2 independent power providers & Internet providers?
    - * cheap power? renewable power? / Enough power? Reliable?
    - * Cabling routes to the building & inside it determined?
    - * Is present in shared building? How reliable is Others used?
  - → Foreign Countries :
    - * country reachable at all times?
    - * corruption? / politically stable? / legal status of data?

* Physical structure
  - → Floor: Must be able to carry 1500 – 2000 kg/m².
    - * Raised floors: metal frameworks carrying tiles, height 40-120 cm
      Disadvantage: Expensive, Height decreased, doors ; eg loading slope hard to install
      Fire can easily spread
  - → Walls, Windows, Doors
    - Walls: Firewall, fire rating
    - Windows: Not desired; If present, should be shatterproof, translucent
    - Doors: Min 1m x min 2.1 m, resist forced entry, fire rating (eg brought in easily), Emergency exit clearly marked, monitored alarmed
  - → Water & Gas Pipes: No leakage
  - → Layout:



→ Storage & spare material

* Power supply (kW - MW)
calculated in kW/m^2. normal density data: → 2-6 kW/m^2
high → 10-20 kW/m^2

UPS (Uninterruptible Power Supply)
Issues with power supply:
→ Blackout (total loss of power) → Surge (A period & high V)
→ Spike (instant jump) → Brownout (voltage drop)
→ Waveform issues

UPS provides high quality electrical power in emergency, & filters the power
UPS Install^n consists of filters, diesel power generator, batteries & flywheel sys

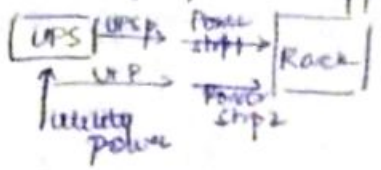
→ Power generators
0.5 - 2MW Power, Diesel should be refilled regularly, loss calorific value
Testing regularly: → Test working of generator
→ Old diesel is used up
→ Use power gen at peak time

→ Battery powered UPS
Batteries last 5-15 minutes, power generator must be started during this period.
3 types -
① standby UPS / off-line systems: used in small setups, provides AC power from battery using electronic inverter
② Line interactive UPS: uses transformer in b/w, works as filter for many power issues, provides AC
③ Double conversion UPS: Convert AC to DC, then back to High Qual. AC using an Inverter. Hence power to IT systems is local & free of power issues. Provides AC from the batteries, which eliminates switch over moments & avoids AC power phase changes.

→ Flywheel UPS
Utility grid to motor rotating a flywheel generating electricity
10-40 sec, 50K-55K rotations/minute.

→ UPS maintenance
→ Batteries: Every 3-5 years → Flywheel → regular bearing repl, upto 30 yrs.
→ Power generator: preheated, monthly testing

→ Power distribut^n
2 types of PDUs: → floor mounted
→ power strips, rack PDUs, feed the rack
Usually redundancy & 2 power supp in comp, 2 power strips.



Knowledge is wealth

SECURITY

(UNIT 5) (1)

Combination of availability, confidentiality & integrity focused on the recognition & resistance of attacks.

Various reasons for comitting crime against IT:
- → personal exposure & prestige
- → financial, damaging org, terrorism, warfare

Risk Management

Process of determining an acceptable level of risk, assessing the current level of risk, taking steps to reduce risk to acceptable level, & maintaining that level.

A risk list used to quantify risks, compiled in Bus Imp. Analysis (BIA) workshop, containing:
- → Asset name: component that needs to be protected
- → Vulnerability: a weakness, process or physical exposure that makes asset susceptible to exploits
- → Exploit: a way to use vulnerabilities to attack an asset
- → Probability: estimate of likelihood of occurence of an exploit
- → Impact: Severity of damage when vulnerability is exploited
- → Risk = P x I

* Controls mitigate these risks

AVE	PIR

→ Risk Response
- → Acceptance of risk: Risk is unlikely & cost of mitigatn is high
- → Avoidance ——
- → Transfer ——
- → Mitigation of risk:
  - → Design for minimum risk
  - → Incorporate * safety devices (Firewalls, Hardened screen routers, Psame but I↓) * warning devices (intrusion detection system, alarm for unusual situ)
  - → Implement training & procedures: mitigate people bound risks

→ Exploits
* key loggers installed (steal password)
* Disposed PCs / disk in wrong hi
* Data on backup tapes outside building in wrong h.
* Corrupt / dissatisfied staff
* N/N sniffers
* End users led to malicious websites stealing info (Phishing)

→ Security controls

Three core goals of security: CIA

→ Confidentiality: prevents unauthorized disclosure of data

→ Integrity: ensures-
* No modifn on data by unauth staff or pr.
* Unauth mod to data not by auth staff or pr.
* Data is consistent

* controls based on risk lists & CIA classifn

→ Availability: reliable & timely access to data or resources by staffs.

cl
rmines what level of CIA needed)

→ Attack Vectors

Attacks on Infra can be executed using:

⇒ Malicious code: App's, when executed can cause n/w or servers overload, steal data & passwords, or erase data

Multiple forms:

→ Worms: self replicating programs that spread from one comp to another

→ Virus: ——— program fragment that attaches itself to a program or file, spreading & leaving infections

→ Trojan horse: appear to be legit files from legit src, hence readers tricked to start them, & then they deliver viruses or worms

* Detecting viruses is done using virus signature, a unique string of bits that identifies a part of the virus.
* Heuristic scanning is also used, which looks for certain instructions or commands within a program that are not found in typical applications. This way viruses can be scanned even before their signature is known to the anti virus s/w vendor.

⇒ Denial of service Attack: attempt to overload an infra to cause disruption of a service. Attacker fires a large no. of malformed req; Usually one computer alone has insuff. power or bandwidth, distributed DOS attack is used.

Prevention:

⇒ split business & public resources
⇒ move public facing resources to external cloud provider
⇒ setup automatic stability
⇒ lower Time to live of DNS Records to reroute traffic to other servers on attack.

Measures on a ddos attack:

⇒ Inform ISP & ask for help
⇒ Run script to terminate connects from same source if >10
⇒ change to an alternative server
⇒ Reroute or drop suspected traffic

CDN can take mitigating actions.

⇒ social engineering: using social skills to manipulate people to obtain info.

⇒ Phishing: email redirecting to seeming legit website asking everything

⇒ Baiting: uses physical media, like USB flash drive, & relies on the curiosity of people to find what is on it.
To mitigate, disable 'auto-run' feature on all org PCs.

(UNIT-5)

* Cooling

Two types of cooling systems:

CRAC : Computer Room ACs : refrigerant based unit connected to outside condensing units

CRAH : ——— Air Handlers : chilled water based & connected to outside chillers.

Metrics for efficiency of cooling sys:

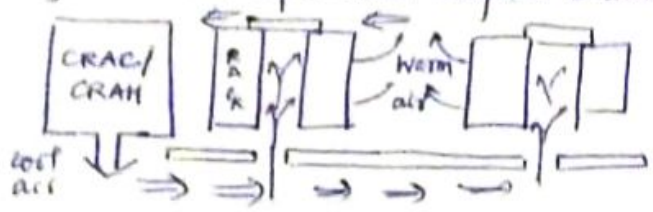
→ EER : eff at max air conditioning load = $\frac{\text{O/P cooling (in BTU) per hr}}{\text{EE I/P in watts}}$

→ SEER : Seasonal EER, seasonal data is used for measurement (time & year cooling sys is most used) = $\frac{\text{O/P cooling (in BTU) in sum}}{\text{EE whrs}}$

→ COP : $\frac{\text{cooling load (KW)}}{\text{EE I/P (KW)}}$ (3-10)

⇒ Operating Temp (18-27°C)

⇒ Airflow : An optimized airflow eliminates hotspots & hence less cooling can do.



⇒ Humidity & Dust :

* Dust should be minimized
* Humidity should be 40-60%.

Dry air can cause Electro static Discharge & loose V in ICs.

Humid air can cause corrosion in printed boards, tape disks can get mechanical problems.

* Fire prevention, detection, suppression

Fire can spread quickly because of air flows & raised floors.

Four levels in suppressing fire:

→ Fire prevention
- Avoid cable spaghetti
- not overloading power

→ Passive fire protection
- Install fire resistant walls
- Wall fire entry pts should be fire resistant (cables, air ducts, coolant tubes)

→ Fire detection
- smoke det
- heat det
- flame det
- alarm
- switch etc

→ Fire suppression
Fire needs Heat, fuel, oxygen
Reduce heat by water X
Replace O_2 by Halon but can dizziness
Now, used Argon

* Gas in datacenter can cause 50% ↑ in pressure → break windows
Hence proper vent needed.

Equipment Racks

Standardized metal enclosures to house IT Infra comp.

Front panel : 19 inches

Height in rack units or 'U' (U = 44.5 mm)
42U generally
Rack mounted servers : 1-2U
blade server enclosures : 10U