Cybersecurity Notes:

Basics

Threats: Most common types of attacks

- Malware(Virus, trojan, worm. Code with malicious intent that steals data or destroys it)
- MitM(Impersonate end points in information exchange.)
- Phishing(Mostly email based. Lure victims into revealing sensitive information.)
- Drive-by downloads(Downloaded from visited website without user action)
- Password attacks(Cracking passwords)
- Maladvertising(Downloaded via infected ads)
- DDoS(Disrupt services. High volume of traffic to overload network)
- Rogue Software(Malware pretending to be legitimate software)

Cybersecurity: What is cybersecurity?

- Used to protect against unauthorised access to data and systems. Protection of internet-connected systems(hardware and software) and data, from cyberattacks.

- Information security: Maintain the confidentiality, integrity and availability of data. Subset of cybersecurity.

- Cybersecurity prevents cyber attacks, data breaches, and identity theft. Aids in risk management.

- Organizations with strong network security and effective incident response plans can better mitigate against and prevent attacks.

->Goal is protection against:

- Unauthorised Access
- Unauthorised Modification
- Unauthorised Deletion

The CIA Triad: 3 pillars of security. Most security policies are based on these.

- **Confidentiality**(Privacy): Measures insure only intended users can access information. May include training for users with access to confidential data, password policies and awareness about social engineering methods.

- **Integrity**(Maintaining the consistency, accuracy and trustworthiness of data over entire life-cycle). Measures ensure data cannot be modified by unauthorised users. May include user access controls and file permissions. Version control may be used to prevent unintended changes to data, inclusion of cryptographic checksum, backups and redundancies.

- **Availability**(Insuring availability of data): Measures ensure data is available and secure. Measures may include maintenance of hardware, regular updating of all software including operating systems, preventing bottlenecks, use of redundancy, fail-over, or high availability clusters, a comprehensive data recovery plan which takes into account natural disasters and secure offsite backups .

Mitigation: 3 main factors:

- **Vulnerability**:An unpatched defect/bug in hardware or software which can be exploited by attackers to cause damage to one of the elements of the CIA triad. Test for vulnerabilities to identify weakpoints and develop a strategy to respond quickly and a data recovery plan.

- **Threat**: Newly discovered incident which can cause harm to systems or organisations. Worms and viruses are categorised as threats.

  - ➔ Natural threats: Floods, earthquakes etc.
  - ➔ Unintentional threats: Employees mistakenly gaining access to the wrong information etc..
  - ➔ Intentional threats: Malware, trojans, spyware etc.

  Conduct threat assessments regularly, ensure users are up to date on latest threats, and conduct penetration tests.

- **Risk**: Potential loss or damage when a threat exploits a vulnerability. Create and implement risk management plan.

  - ➔ Assess risk
  - ➔ Determine needs
  - ➔ Include total stakeholder perspective

3 steps in mitigation:

- Identify the threat or activity
- Analyse and evaluate all affected parties and compromised systems
- Treat the threat and return to normal operations

Incident Response:

Detection and Mitigation Software:

- **ARP: (**Activity Response Software/Process)
  - ➔ Monitors users and processes in the network

  - Alerts SIEM system in case of unusual activity
  - Uses Threat Intelligence Software to flag suspected IP addresses
  - Generates playbooks for incident responders
  - Detects vulnerabilities exploited in attacks and which systems have been compromised

- **SIEM:** (Security Information and Event Management System)
  - Analyses alerts from ARP
  - Detects unusual activity/behaviour
  - Logs events
  - Generates reports

Role of Incident Response Team/Analyst:

- Take mitigation measures against the attack
- Attempt to limit the extent of the damage caused by the attack
- Detect the extent of the damage done by the attack. What data was compromised? How many users are affected? Etc.
- Contact regulatory agencies to notify them about the users affected in their jurisdictions.