CYBER ENRICH TRAINING PROGRAM | MODULE II

Cyber Security

Cyber Security

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks.

Why do we need Cybersecurity?

Economic Costs

- Cybercrimes generally have irreparable effects on the overall economy of the business
- In 2019, over $1 Trillion were lost due to cybercrimes, equal to Australia's nominal GDP

Reputational Costs

- They greatly harm aspects like customer loyalty and new customer acquisition, resulting in an eventual loss
- Huawei was banned from selling its products in North America because it was alleged of spying on its users

Regulatory Costs

- They may have to pay fines and sanctions set by government authorities in case of a data breach
- Uber paid $148 Million in fines in 2018 to the US government due to a data breach

Where do Cyber attacks come from?

48% of malicious email attachments are office files

34% of data breaches involved internal actors

65% of groups used spear-phishing as the primary infection vector

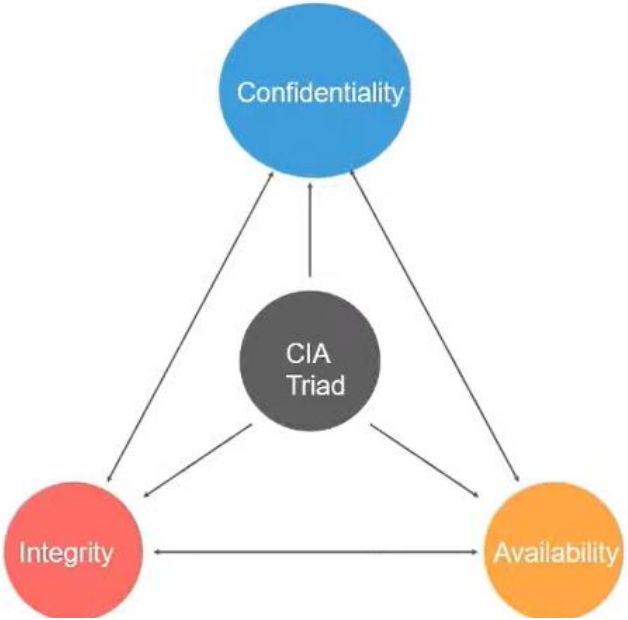
94% of malware was delivered by mail

Where do Cyber attacks come from?

Protection is the mechanism used to control the access of system/network resources, programs, and processes.

The CIA Triad

CIA Triad is the model designed for developing policies to provide security to an organization



Confidentiality **C** The system should restrict unauthorized access to the information.

Integrity **I** The system has to perform all its functions without being affected by its internal or external environment.

Availability **A** The system should be available to authorized user trying to access it during the time it is supposed to be available.

Attacks on CIA

Confidentiality

- Cracking Encrypted Data
- Man In The Middle attacks on plain text
- Data leakage/ Unauthorised copying of sensitive data
- Installing Spyware/Malware on a server

Integrity

- Web Penetration for malware insertion
- Maliciously accessing servers and forging records
- Unauthorised Database scans
- Remotely controlling zombie systems

Availability

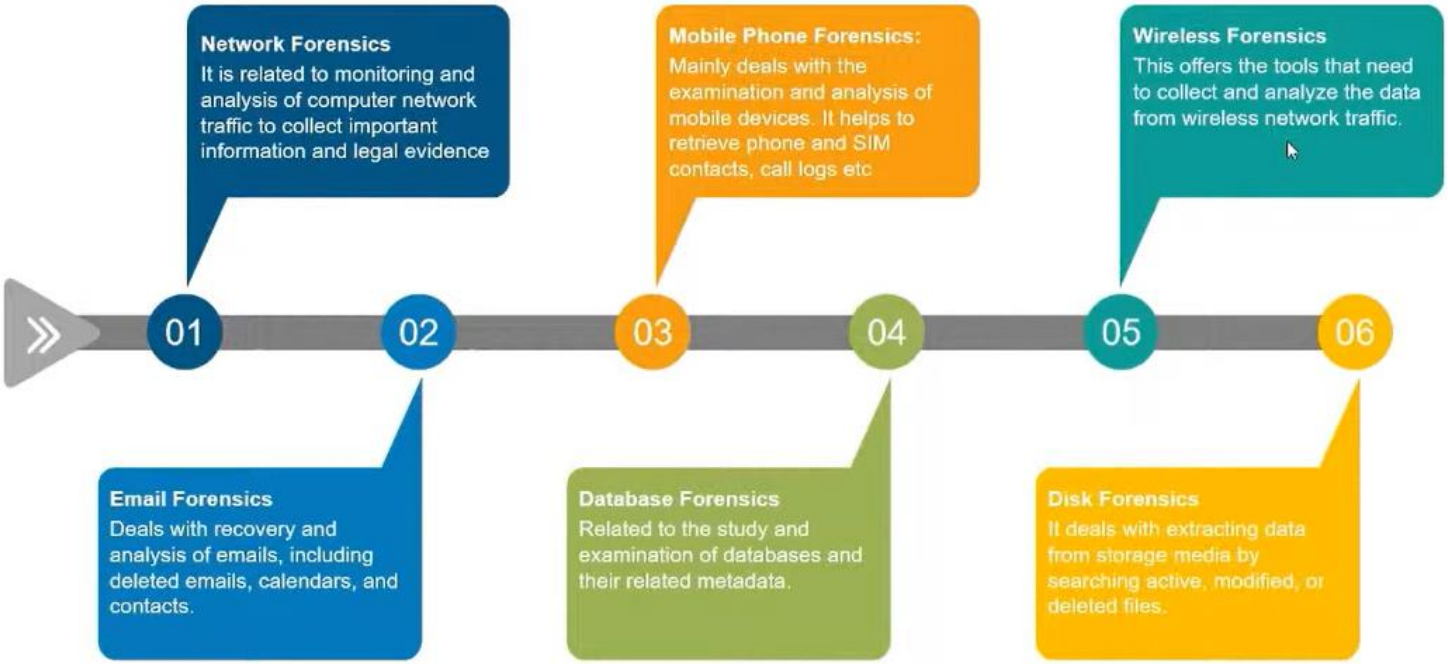
- DOS/DDoS attacks
- Ransomware attacks – Forced encryption of Key data
- Deliberately disrupting a server rooms power supply
- Flooding a server with too many requests

- ✓ Digital forensics is the process of identifying, preserving, analysing, and documenting digital evidence.
- ✓ This is done in order to present evidence in a court of law when required.

What is Digital Forensics in Cybersecurity?

Process of Digital Forensics

Types of Digital Forensics



Applications of Digital Forensics

- Crime prevention
- Supplementary evidence gathering
- Digital crime recognition
- Exoneration
- Position tracking

Advantages

- Helps to protect the organization's money and valuable time
- Ensure the integrity of the computer system
- Allows to extract, process, and interpret the factual evidence.

Disadvantages

- Need to produce authentic and convincing evidence
- Electronic records and storing them are costly