**Terms :**

* Data
* Information System
* Security
* Unauthorized Access
* Privacy
* Cracking Passwords

**Unstructured Data** – stored in the storage

**Structured Data** – stored in the database

**LMS** – Learning Management System

**Three controls** – defense in depths

**TOR Browser** – used to access dark web

**SOC** – Security Operations Center

**Hacking** – Attack a target system without the permission and acknowledgement of the target

**Ethical Hacking** - Hacking a target system with full permissions of the target

**Two types of hacking :**

* Offensive
* Defense

**Offensive** – hacking etc…

**Defensive** – Forensic etc…

If the difference between **Vulnerability**, **Risk** and **Threats** is known then cybersecurity or hacking is easy

**Vulnerability** – gateway (or) end point

**Severity** – damage

If Vulnerability is linked to threat that post the security risk. If it is not linked then no security risk

**HACKERS** – Threat Actor / Adversaries / Bad Actor

The hack for financial gain, political gain, DOS attack (or) competitive

**Types Of Threats :**

* Insider Threat
* Outsider Threat

**Insider Threat :**

Working in an organisation and hacking that same organization

**Outsider Threat :**

Third party threats

**APT** – Advanced Persistent Threat :

Attacker has the access to the system for a very long time or else once the system closes and when opened the IP address is changed

Password is also known as the **Passphrase**

**Hackers follow five steps to hack :**

* Information Gathering – gather lots of information about the target
* Scanning – find open ports, technologies like HTML, Java, HTTP, HTTPS etc…
* Gaining Access
* Persistence / Maintaining Access
* Cleaning Digital Footprints