Dated 8/30/2022 BWL DAY#1

**1. WHY DO WE NEED CYBER SECURITY?**

**2. What is CYBER SECURITY?**

**3. CIA TRIAD**

**4. VULNERABILITY, THREAT, and RISK**

**5. COGNITIVE CYBER SECURITY?**

We are living in the age of digitalization, where data is stored on a cloud server or data center which can be easily accessed online from different devices.

**The golden age for data exploits**

It’s a golden age for black hat hackers with so many IP addresses, Access points, constant traffic, and a lot of data to breach.

Black hat hackers exploit vulnerabilities and create malicious software for different organizations to make them a victim of cyberattack.

**Common types of cyber threats**

* MALWARE
* Man in the middle (MITM)
* Phishing
* Drive by Download
* Password Attacks
* Maladvertising
* DDOS(Daniel of service)
* Rogue Software

Cyber security is the protection of internet connection systems, including hardware, software, and data, from cyber attacks. types of security as per enterprises:

1. Cyber security
2. Physical security

Cyber security protects against:

* Unauthorized Modification
* Unauthorized Deletion
* Unauthorized Access

**CIA triad**

Confidentiality, Integrity and Availability

**Confidentiality = data must be completely secure and protected**

**ATTACKS ON CONFIDENTIALITY**

* Cracking encrypted Data
* Data leakage/unauthorized copying of sensitive data
* Installing Spyware / Malware on a server

**Integrity = data must not be changed by any person**

**ATTACKS ON INTEGRITY**

* Web penetration for malware Insertion
* Maliciously accessing servers and forging records
* Unauthorized Database scans
* Remotely controlling zombie systems

**Availability = Data is available to the right person**

**ATTACKS ON AVAILABILITY**

* DOS/DDOS attacks
* Ransomeware attacks
* Deliberately disrupting a server rooms power supply
* Flooding a server with too many requests

**Steps to fix a cybercrime**

1. Identify
2. Analyze and evaluate
3. Treat

**Vulnerability**

It refers to the weakness of an asset that can be exploited by an attacker.

**Threat**

A threat is any event that has the potential to bring harm to an organization or individual.

**Risk**

Risk refers to the potential for loss or damage when a threat exploits a vulnerability.

**SIEM Working**

Security information and event management help organizations detect, analyze, and respond to security threats before they harm business operations.

**Patching**

Cyber security analyst uses ARP (address resolution protocol) and identifies and patches all the thing ARP uses information from endpoint tools to determine which machine needs to be patched. Recommends how to patch them and allows to put the patches to all the computers and mobile devices instantly.