Definition of Cybersecurity

Security in computer technology comprises cybersecurity and physical security. Cybersecurity is also referred to as information technology security.It refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber attacks are usually aimed at accessing, changing, or destroying sensitive information.Another type of attack is extorting money from users; or interrupting normal business processes.
Surprisingly Cybersecurity doesn't have a trademark and neither it is owned by anyone as in the case of Bluetooth, Wi-Fi.The normal expression is" Everyone owns cybersecurity"

Following elements of cyber technology need Cybersecurity

1.Network security- A strategy that enables guaranteeing the security of its assets including all network traffic. It includes both software and hardware technologies. Wireless networks can be subject to vulnerability, malicious eavesdropping, hacking, and freeloaders. Hackers are increasingly becoming smarter day by day.
The need to utilize a network security tool becomes more and more impotent. Following type of network security tools are very important to save from attackers. Antivirus and Antimalware Software- Malware, which includes spyware, ransomware, Trojans, worms, and viruses are very dangerous. They can infect a network. This software handles this threat by scanning for malware and regularly track files in order to detect anomalies, remove malware, and fix the damage.
2. Application security-Application security is the use of software, hardware, and procedural methods to protect applications from external threats. All the Apps are not created perfectly. It is possible for any application/app to comprise of vulnerabilities, or holes, that are used by attackers to enter the network. Application security software, hardware, and processes are used to close those holes.
3. Endpoint security (Endpoint Protection) –Also called Network Security refers to the approach of protecting a business network when accessed by remote devices like smartphones, laptops, tablets or other wireless devices. Each device with a remote connecting to the network creates a potential entry point for security threats. Endpoint security is designed to secure each endpoint on the network created by these devices.
4. Data security-It refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases, and websites Identity management. Data security is the process of securing the data and protecting it from unauthorized and corrupted access. There are many ways to protect data, and some of them include strong user authentication, encryption, data

erasure, backup, etc.
5.Database security-Refers to database management software from illegitimate use and malicious threats and attacks. the database server should be protected from database security threats by a firewall and web application firewall.
6.infrastructure Security-The security measures to protect infrastructures, especially critical infrastructure, such as network communications, communication center, server center, database center, and IT center. Infrastructure security seeks to limit the vulnerability of these structures and systems from sabotage, terrorism, and contamination.
7. Cloud security-Refers to a set of policies, controls, procedures, and technologies that work together to protect cloud-based systems, data, and infrastructure. Procedures are designed to stop unauthorized data exposure and leaks, weak access controls, susceptibility to attacks,
8.Mobile security-Refers to protection from threats and vulnerabilities associated with wireless computing. Mobile security is also known as wireless security. Mobile security involves protecting both personal and business information stored on and transmitted from smartphones and other mobile devices.
9. Disaster recovery/business continuity planning-Business continuity planning is a strategy. It ensures continuity of operations with minimal service outage or downtime. A business disaster recovery plan has the capability to restore data and critical applications in the event your systems are destroyed when disaster strikes
10.End-user education-Refers to awareness to identify many of the common risks associated with using conventional end-user technology. It has been found the end user within the organization is often the first to compromise security. The prevention includes educating employees that they will be targeted, encouraging them to be vigilant at all times. Employees are taught what qualifies as sensitive data, how to identify and avoid threats.