Cyber Security:

The only system which is truly secure is one which is switched off and unplugged locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it.

There is nothing like absolute security. We are only trying to build comfort levels, because security costs money. Also, Internet allows an attacker to work from anywhere on the planet.

Cyber:

Cyber refers to the technology that includes systems, networks, programs, and data. These Technologies include servers, laptops, smartphones, smart TVs, webcams, and even vehicles. Cyber means anything that is digital. It can be your devices that are performing the digital computation. Anything that is related to the Internet falls under the category of Cyber.

Security:

Security is concerned with the protection of systems, networks, applications, data and information. We must protect our computers and data in the same way that we secure the doors to our homes. The word comes from Latin, meaning free from care. Sometimes security is defined as the state of being free from danger, which is the goal of security. It is also defined as the measures taken to ensure safety, which is the process of security. Security can be defined as the necessary steps to protect from harm.

Cybersecurity:

There are several definitions of Cybersecurity.

Cybersecurity is the protection of internet-connected systems, including hardware, software and data from cyberattacks. Cyber Security is the protection of information systems and organizations against cyber threats.

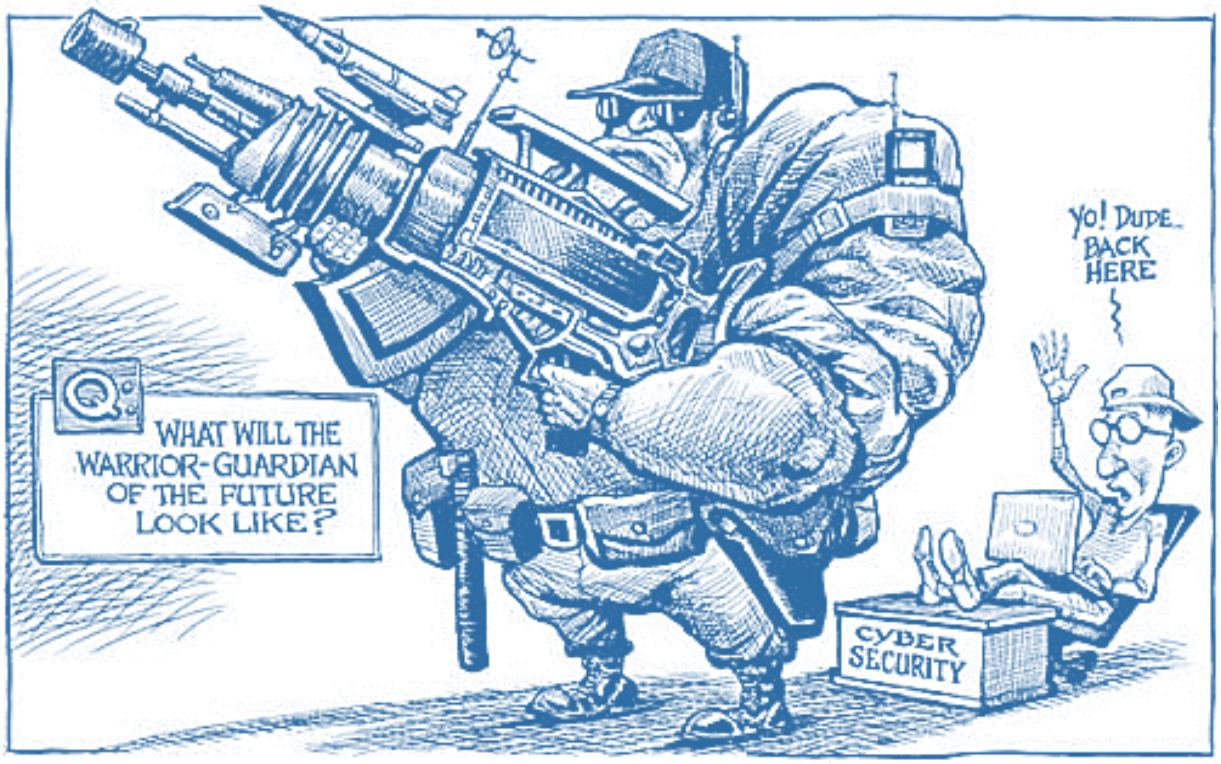
Cybersecurity is the set of tools, risk management approaches, technologies, training, and best practices designed to protect networks, devices, programs, and data from attacks or unauthorized access. Set of principles and practices designed to protect our computing resources & online information against threats.

Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access. The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.

Cybersecurity OR Cyber Security:

American style tends to favor cybersecurity as one word while British style often uses cyber security as two words. Cybersecurity and cyber security have the same meaning.

Cybersecurity is like an arms race with both sides constantly evolving their weapons and defenses. You need to continuously evolve your security strategy, or you might get left behind in the race, holding a sword and shield to protect yourself against a fighter jet.



On one side, hackers are coming up with new phishing techniques, creating new & increasingly dangerous types of malware every day, constantly setting traps for victims to get caught up in, and searching for new vulnerabilities to exploit.

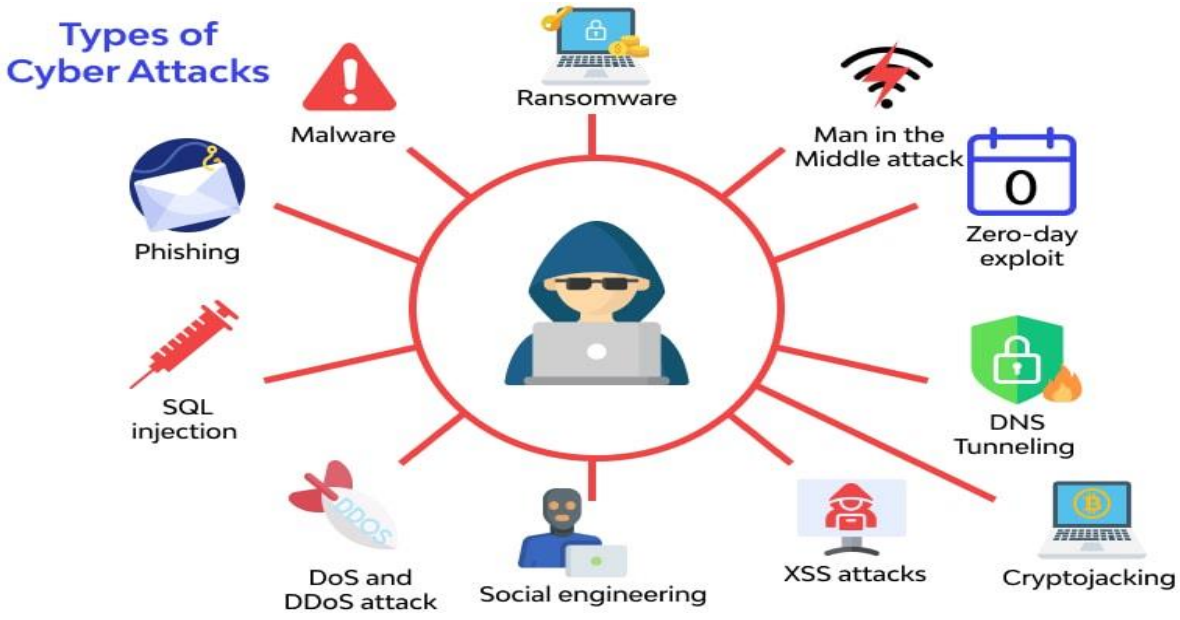
On the other side, the good guys need to develop measures to protect against new threats, continuously update security software definition files, patch software and OSes regularly, stay vigilant when on the web, and educate everyone in their organization about new threats, so they won't fall victim to them.

Attack:

Attack can be defined as action taken by an attacker to harm an asset such as system, network and data. An attack is when an unauthorized person is able to access your system or data without your knowledge. An attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset. Most attacks take place whenever a part or more of your system are vulnerable or not properly secure.

Cyberattacks:

Cyberattacks are malicious attempts to access or damage a computer or network system. A cyber-attack is an exploitation of computer systems & networks. Cyberattacks are unwelcome attempts to steal, expose, alter, disable or destroy information through unauthorized access to computer systems. The person who carries out a cyberattack is hacker or attacker. By some counts, there are more than 2,200 cyberattacks per day. About one cyberattacks every 39 sec.



Types of Cyberattacks:

There are many varieties of cyber-attacks that happen in the world today. While there are many different ways that an attacker can penetrate an IT system, most cyber-attacks rely on pretty similar techniques. If we know the various types of cyberattacks, it becomes easier for us to protect our networks and systems against them. Here are different types of cyberattacks.

MAC Flooding Attack, DoS Attack, DDoS Attack, SYN Flooding Attack, DHCP Attack, Man-in-the-Middle Attack (MITM), SQL Injection Attack, DNS Attack, STP Attack, Phishing Attack, VLAN Hopping Attack, CDP Attack, ICMP Flooding Attack, UDP Flooding, Buffer Overflow, ARP Spoofing Attack, Malware Attack, Password Attack, Smurf Attack, Ping of Death Attack, IP Spoofing, Cross Site Scripting, Brute Force Attack and more.