1. **What are the 6 ethical issues to consider in Cybersecurity?**

* *Privacy*

Protecting individuals' personal data from unauthorized access, use, or sharing is a major concern. Cybersecurity professionals must ensure that systems uphold users' privacy rights.

* *Data Integrity*

Ensuring data is accurate, consistent, and unaltered is critical. Altering or tampering with data—especially in healthcare, finance, or legal records—can have serious ethical implications.

* *Security vs. Freedom*

There's often a tension between maintaining security (e.g., surveillance, data monitoring) and respecting individual freedoms (e.g., free speech, anonymity). Ethical cybersecurity must balance these concerns.

* *Responsibility and Accountability*

Cybersecurity professionals must be accountable for the tools they create or manage. Misconfigurations or negligence that lead to breaches raise ethical questions about professional duty and liability.

* *Hacking and Unauthorized Access*

Even for ethical purposes (like white-hat hacking), gaining unauthorized access to systems can pose ethical dilemmas—especially if done without informed consent or legal clearance.

* *Bias and Fairness in Algorithms*

Security systems using AI or automation must be free from bias. Discriminatory practices in intrusion detection or surveillance can unfairly target specific groups or individuals.

1. **What is denial of services or DOS**

A Denial of Service (DoS) attack is a type of cyberattack that aims to make a computer system, website, or network resource unavailable to its intended users by overwhelming it with excessive traffic or triggering a crash.

1. **Name 5 issues with Cybersecurity**

* *Data Breaches*

Sensitive data (personal info, financial records, etc.) can be stolen due to poor security practices, weak passwords, or system vulnerabilities.

* *Phishing Attacks*

Cybercriminals trick users into revealing personal information or clicking malicious links by pretending to be trusted sources via email or messages.

* *Ransomware*

Malware that locks users out of their systems or files until a ransom is paid. It's a growing threat affecting individuals, businesses, and governments.

* *Insider Threats*

Employees or trusted individuals misusing their access—either intentionally or accidentally—can cause serious damage to systems and data.

* *Outdated Software and Systems*

Using outdated or unpatched software leaves systems vulnerable to known exploits and attacks.

1. **What are the 5 issues in data level with the regards to Cybersecurity**

* *Data Breaches*

Unauthorized access to confidential or sensitive data—often due to weak security controls—leading to exposure, theft, or misuse of information.

* *Data Integrity Violations*

Data can be altered, corrupted, or tampered with—intentionally or accidentally—undermining its accuracy and trustworthiness.

* *Data Loss*

Important data may be deleted, overwritten, or lost due to system failures, human error, or malicious attacks, especially without proper backups.

* *Unauthorized Data Access*

Users accessing data they are not permitted to see or modify, often due to poor access control policies or insider threats.

* *Improper Data Classification*

Failing to label or categorize data correctly (e.g., public, confidential, restricted) can lead to improper handling, sharing, or storage—putting sensitive data at risk.