1. Social Threats

- **Phishing**: Deceptive emails or messages designed to trick users into providing sensitive information or downloading malicious software.
- **Spear Phishing**: Targeted phishing attacks directed at specific individuals or organizations, often using personalized information.
- **Social Engineering**: Manipulating individuals into divulging confidential information or performing actions that compromise security.
- **Pretexting**: Creating a fabricated scenario to trick a victim into revealing information or performing an action.
- **Baiting**: Offering something enticing to lure victims into a trap, such as a USB drive loaded with malware.
- **Quid Pro Quo**: Promising a service or benefit in exchange for information, often used in social engineering.

2. Technical Threats

- **Malware**: Software designed to disrupt, damage, or gain unauthorized access to computer systems (e.g., viruses, worms, trojans).
- **Ransomware**: A type of malware that encrypts files and demands a ransom for their decryption (e.g., WannaCry).
- **DDoS (Distributed Denial of Service)**: Overloading a system with traffic to make it unavailable to users.
- **SQL Injection**: Exploiting vulnerabilities in web applications to execute malicious SQL statements and access or manipulate databases.
- **Man-in-the-Middle (MitM) Attack**: Intercepting and altering communications between two parties without their knowledge.
- **Zero-Day Exploit**: Attacking a vulnerability that is unknown to the vendor or has no patch available.
- **Cross-Site Scripting (XSS)**: Injecting malicious scripts into web pages viewed by other users.
- **Credential Stuffing**: Using compromised credentials from one service to access other services, relying on users reusing passwords.

3. Physical Threats

- **Theft of Devices**: Stealing physical devices such as laptops, smartphones, or servers that contain sensitive information.
- **Tailgating**: Gaining unauthorized access to a secured area by following an authorized person without proper authentication.
- **Dumpster Diving**: Searching through trash to find discarded sensitive information that can be used in an attack.

- **Shoulder Surfing**: Observing someone's actions, such as typing a password, to gain unauthorized access.
- **Tampering**: Physically altering devices or hardware to introduce vulnerabilities or compromise systems.
- **Sabotage**: Deliberate physical destruction or disruption of equipment, networks, or infrastructure.

4. Operational Threats

- **Insider Threat**: A current or former employee, contractor, or partner who misuses their access to an organization's assets.
- **Policy Violations**: Ignoring or circumventing security policies and procedures, leading to vulnerabilities.
- **Configuration Errors**: Misconfiguring systems, networks, or applications, creating security weaknesses (e.g., leaving default passwords).
- **Data Leakage**: Unauthorized transfer or exposure of sensitive information, whether intentional or accidental.
- **Third-Party Risk**: Security risks introduced by vendors, suppliers, or other external partners with access to the organization’s systems.
- **Poor Patch Management**: Failing to apply software updates and patches, leaving systems vulnerable to known exploits.
- **Supply Chain Attacks**: Compromising systems by attacking the software, hardware, or services provided by third parties.