

Storage on an **insecure** medium

➔ Threat 1: **Loss**

An attacker can corrupt or destroy data at rest

➔ Threat 2: **Disclosure**

An attacker can disclose data at rest to other unauthorized parties

➔ Threat 3: **Theft**

An attacker can obtain and store data at an arbitrary location

➔ Threat 4: **Modification**

An attacker can compromise the integrity of data at rest

Storage on an **insecure** medium

➔ Threat 1: **Loss**

Cryptography cannot be used to prevent loss. It may be used to yield loss. E.g ransomware

➔ Threat 2 & 3: **Disclosure & Theft**

Encrypted data at rest cannot be meaningfully disclosed or utilized without decryption. E.g PGP Whole Disk Encryption

➔ Threat 4: **Modification**

Cryptography can be used to verify the integrity of data at rest