4) Employee Sabotage  
This relates to computer threats that occur when employees delete important data files, put viruses on computers with the intention of destroying programs or may even be as simple as entering data incorrectly into a program with the goal of corrupting the integrity of the system

5) Loss of Infrastructure  
Power failures, loss of communication and floods pose a serious threat to computer systems.

6) Personal privacy  
The accumulation of vast amounts of electronic information about individuals by private companies and governments have created a threat to individual privacy

**Vulnerabilities** are weaknesses in computer and security systems, procedures, design or implementation that might be exploited to cause harm or damage

Common Sources of Vulnerabilities

* Files – these play an essential role to any computer system and any damage or theft can lead to system compromise
* Remote Access – the need to share information means that a communication network has to be present which creates the vulnerability of unwanted access
* Cabling/Wiring – they are vulnerable to physical tampering
* Hubs/Switches – these and any hybrid connectors can easily be tampered with and bring down the network

Security Goals

Availability – insuring our information and infrastructure are available to legit users at all times

Confidentiality – ensuring even if an unauthorised person gets access to our info, they won’t be able to understand it unless additional info is provided

Integrity – ensuring data is transmitted in a way that when the receiving party … (missed this note)

Authorization – the process of ensuring appropriate use of resources by authorized users

Authentication – the process of verifying that the communicating party is who they claim to be

Non Repudiation – a process that guarantees the sender of a message cannot later deny having sent the message and the recipient cannot deny receiving it.