# Intro to Security

## Why Need Security?

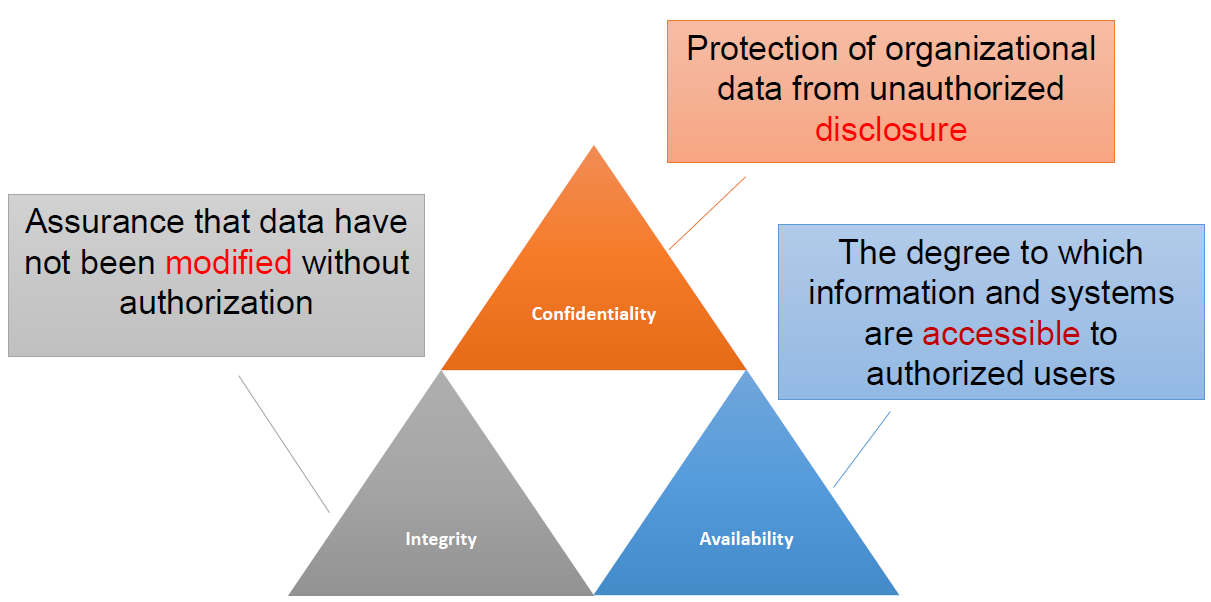
* Reliance on the use of electronic-based information processing, storage, and communication
* Day to day operations depend on the data and applications
* Data is now recognized as the most valuable asset
  + Average value of organizational data and applications far exceeds cost of networks
* Organizations vulnerable due to dependency on computing and widely available Internet access to its resources

## Difficulties in Defense

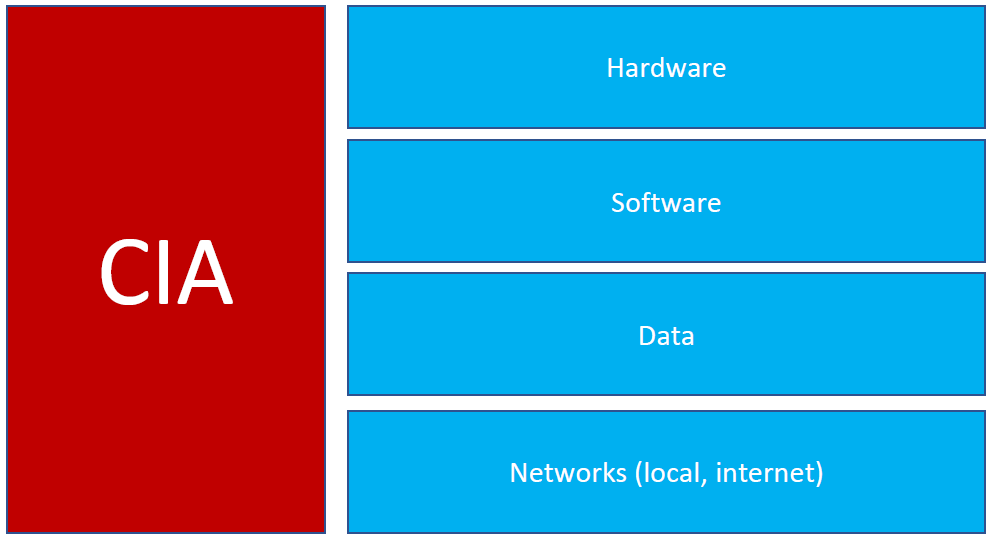
* Universally connected devices means **distributed attacks**
* **Increased speed of attacks**
  + Can scan millions of devices to find weaknesses
  + Automated attack possible without human
* **Greater sophistication of attacks**
  + Complex and difficult (often exploiting internet protocols and applications) to detect and defense
* **Availability of attack tools:** cheap and simple to use
* **Delays in security updating (patches):** Speed of new & modified virus spread is faster than security updates
* **User confusion:** Little or no information to guide users to make security decisions

## Goals of Security: CIA Triad

* **Confidentiality**: protection of organizational (or any other confidential) data from unauthorized disclosure; can be achieved through encryption
* **(Data) Integrity**: assurance that data may not have been **altered** (without authorization), either maliciously or by accident.
* **Availability**: The degree to which information and systems are accessible to authorized users
* **Related terms**:
  + **Authentication** – proving who you are (did you send that message?)
  + **Authorization** – checking if allowed to access an asset usually based upon who you are, something you know or something you possess (can I read Julian’s messages?)
  + **Non-repudiation** – cannot deny knowledge of an action done by a user (I never sent that message to Julian)



## What we are trying to protect



## Vulnerabilities, Threats, Attacks

* Categories of system resource vulnerabilities
  + Corrupted (loss of Integrity)
  + Leaky (loss of Confidentiality)
  + Unavailable or very slow (loss of Availability)
* Security threats
  + Capable of exploiting vulnerabilities
  + Represent potential security harm to an asset
* Security attacks
  + Passive – attempt to learn or make use of information from the system that does not affect system resources
  + Active – attempt to alter system resources or affect their operation
  + Insider – initiated by an entity inside the security parameter
  + Outsider – initiated from outside the perimeter