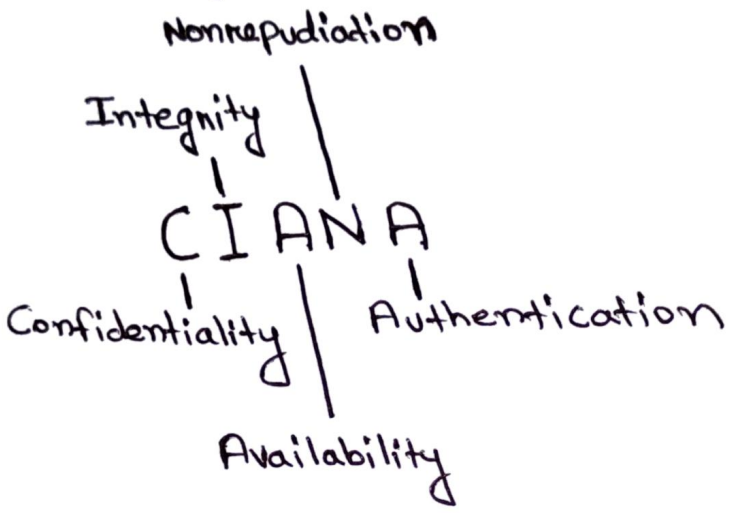
IA → Information Assurance [Organizational Security]

Five Properties of Information Assurance:



Confidentiality → Information is available to those who are authorized and hidden from the one's unauthorized.

The "need to know" principle enforced in military is as following: "Even if one has all the necessary approvals to access certain information, one would not be given access to such information, unless one has a specific need to know; that is access to the information must be necessary to conduct one's official duties."

Example: Encrypting an income tax returns will prevent anyone from reading it and if the owner needs to see the return, it must be decrypted.

Here, a key is used for decryption and if the key is compromised, the confidentiality is destroyed!

Nonrepudiation → It is the assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

In physical world we use handwritten signatures but we have digital signatures too for Cyber world.

Authentication → The process or action of verifying the identity of a user or process. Password is the most common method of authentication.

Authentication is slightly different from authorization.

Authentication = username + Password (who you are)

Authorization = Permissions (what you are allowed to do)

↳ Access Control

Authentication comes first then authorization.

Risk = Likelihood x Impact

(we are actually not going to multiply anything, but it gives an idea. If either of these factors increase, so does the risk!)

Likelihood is a function of threats and vulnerabilities.

A vulnerability is a weakness or defect in a system that maybe exploited to do a bad stuff.

A threat is an actor who has the potential and motivation to do bad stuff.

A vulnerability in the absence of threats is no problem (for example, it does not matter that Superman is vulnerable to kryptonite if there are no bad people that have access to kryptonite)

Similarly, threats are no consequence to an invulnerable system (for example, mean kids with water guns are not a problem for the adults).