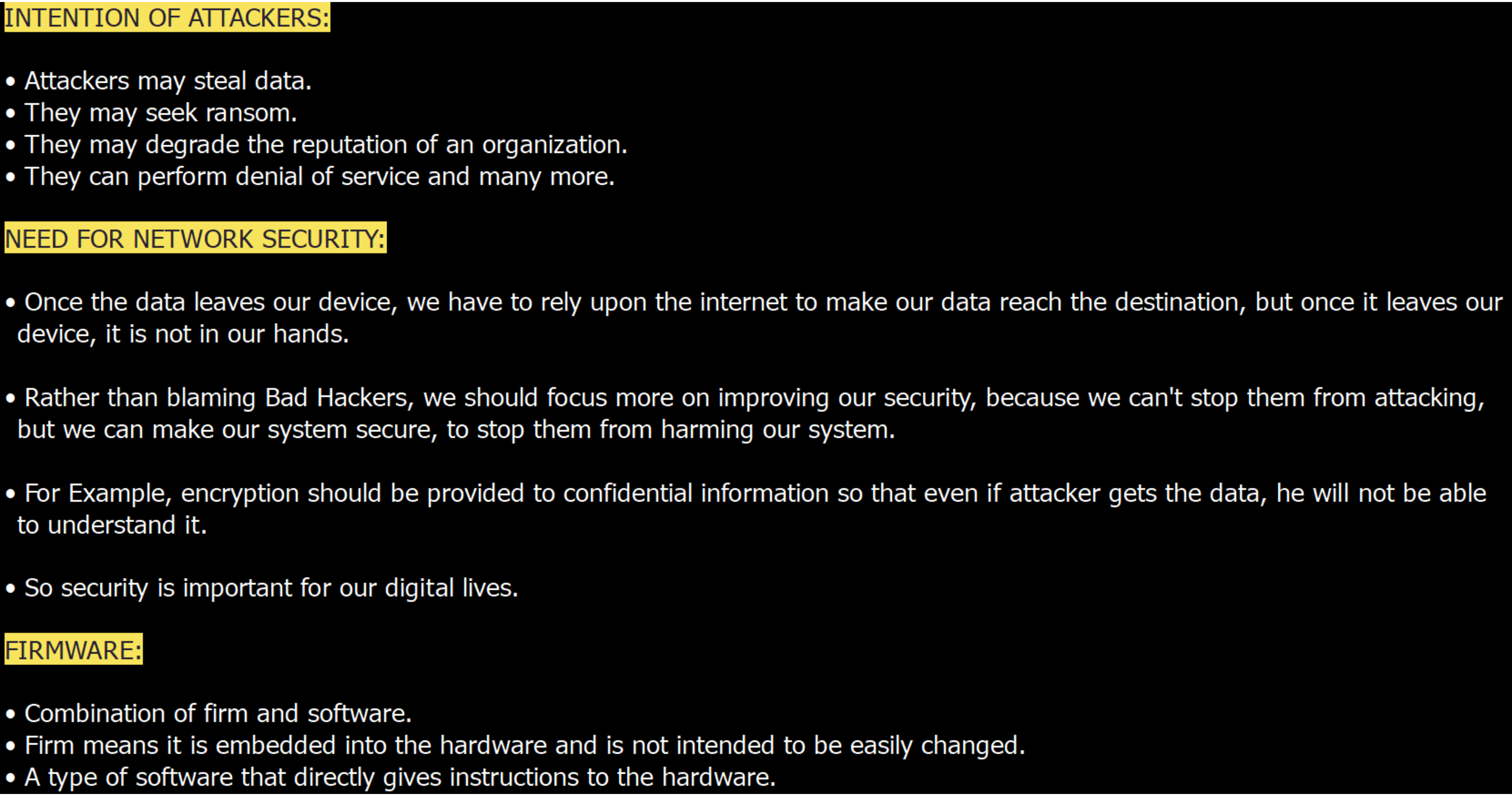


INTENTION OF ATTACKERS:

- Attackers may steal data.
- They may seek ransom.
- They may degrade the reputation of an organization.
- They can perform denial of service and many more.

NEED FOR NETWORK SECURITY:

- Once the data leaves our device, we have to rely upon the internet to make our data reach the destination, but once it leaves our device, it is not in our hands.

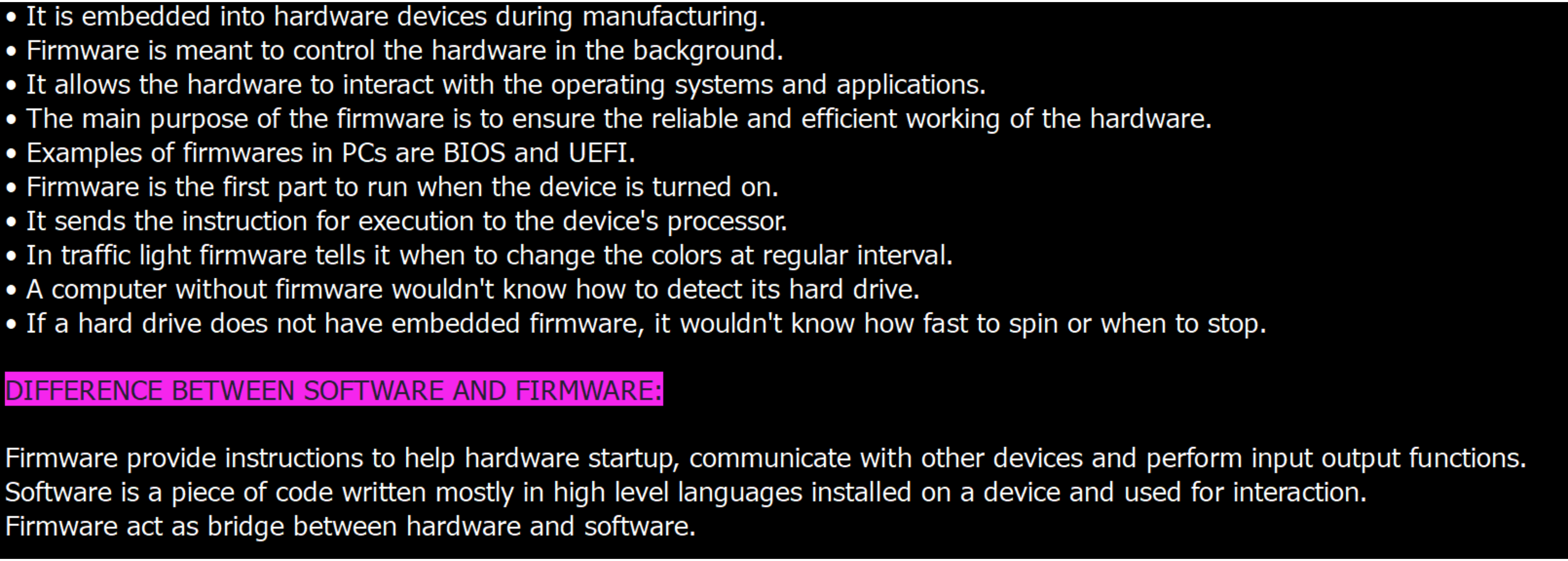
- Rather than blaming Bad Hackers, we should focus more on improving our security, because we can't stop them from attacking, but we can make our system secure, to stop them from harming our system.

- For Example, encryption should be provided to confidential information so that even if attacker gets the data, he will not be able to understand it.

- So security is important for our digital lives.

FIRMWARE:

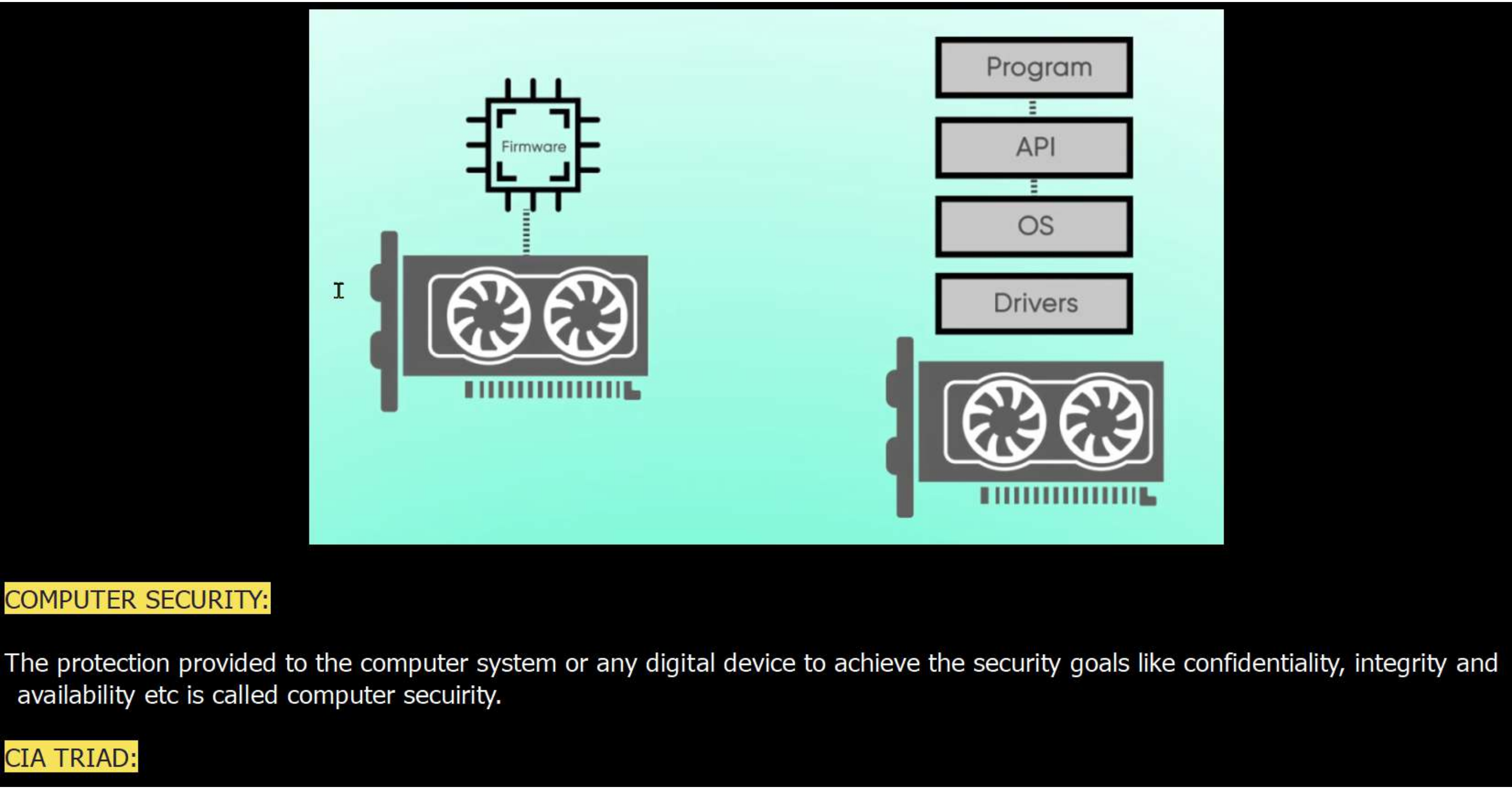
- Combination of firm and software.
- Firm means it is embedded into the hardware and is not intended to be easily changed.
- A type of software that directly gives instructions to the hardware.



- It is embedded into hardware devices during manufacturing.
- Firmware is meant to control the hardware in the background.
- It allows the hardware to interact with the operating systems and applications.
- The main purpose of the firmware is to ensure the reliable and efficient working of the hardware.
- Examples of firmwares in PCs are BIOS and UEFI.
- Firmware is the first part to run when the device is turned on.
- It sends the instruction for execution to the device's processor.
- In traffic light firmware tells it when to change the colors at regular interval.
- A computer without firmware wouldn't know how to detect its hard drive.
- If a hard drive does not have embedded firmware, it wouldn't know how fast to spin or when to stop.

DIFFERENCE BETWEEN SOFTWARE AND FIRMWARE:

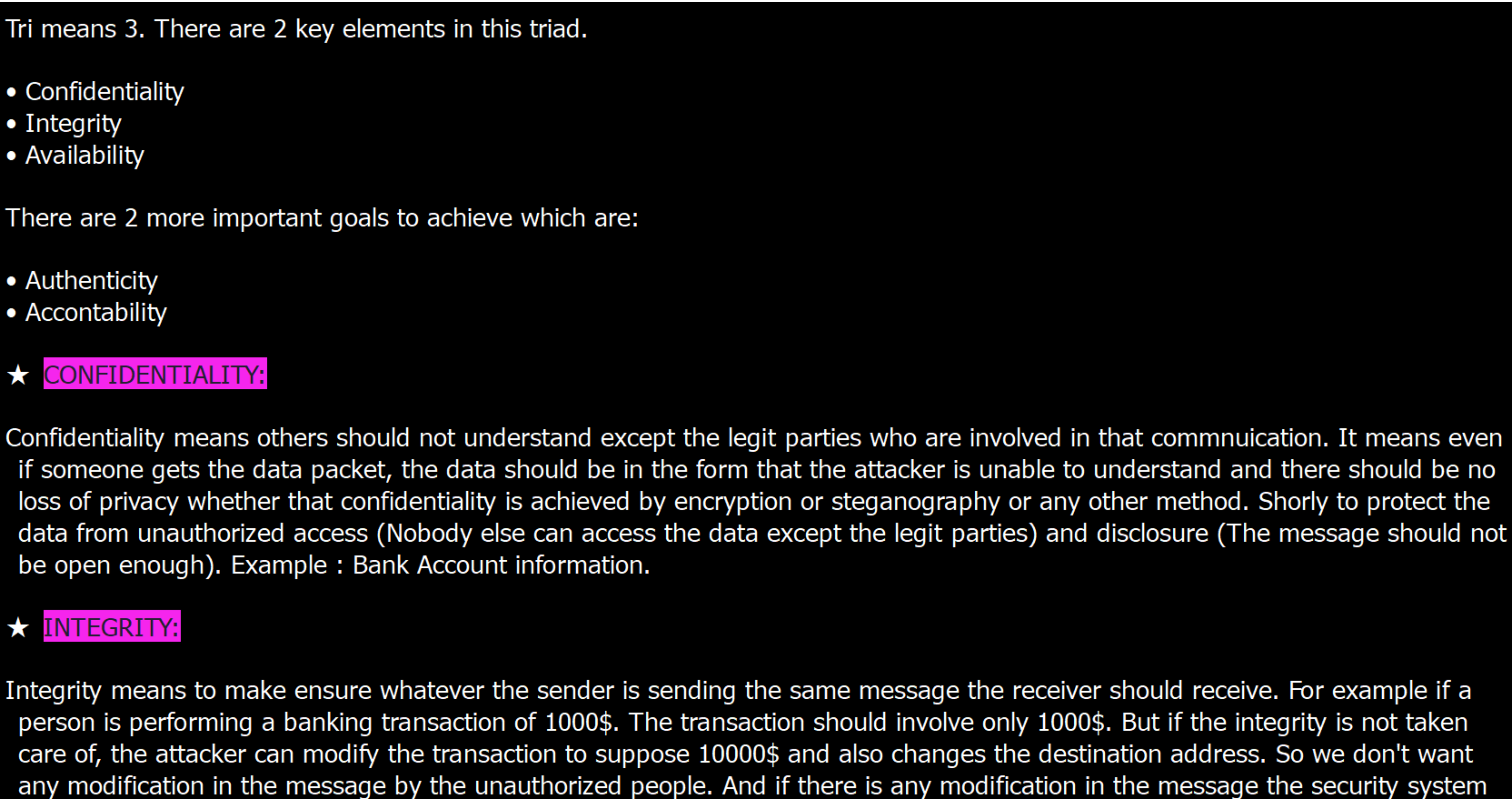
Firmware provide instructions to help hardware startup, communicate with other devices and perform input output functions.
Software is a piece of code written mostly in high level languages installed on a device and used for interaction.
Firmware act as bridge between hardware and software.



COMPUTER SECURITY:

The protection provided to the computer system or any digital device to achieve the security goals like confidentiality, integrity and availability etc is called computer secuirity.

CIA TRIAD:



Tri means 3. There are 2 key elements in this triad.

- Confidentiality
- Integrity
- Availability

There are 2 more important goals to achieve which are:

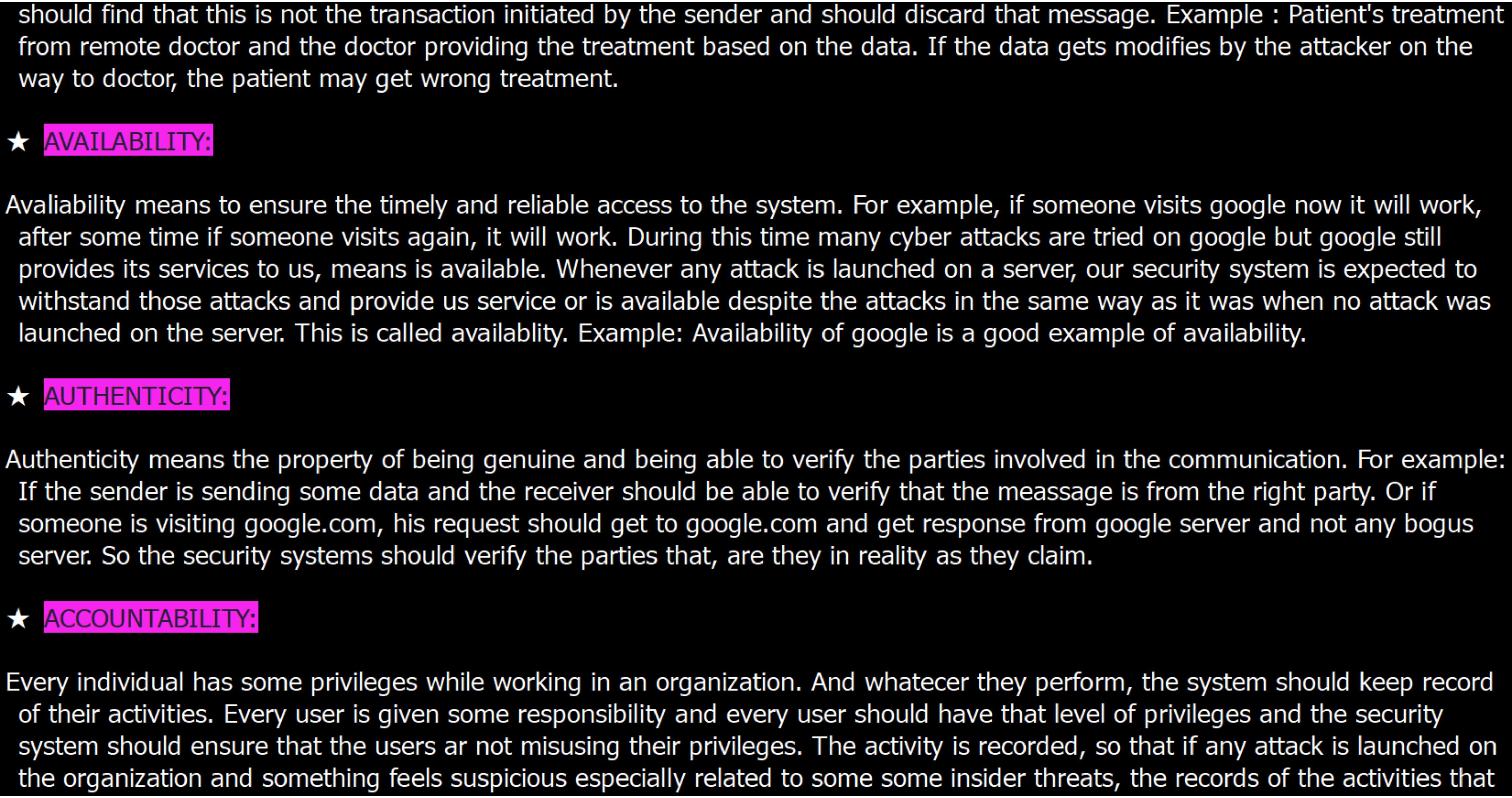
- Authenticity
- Accontability

★ CONFIDENTIALITY:

Confidentiality means others should not understand except the legit parties who are involved in that commnuication. It means even if someone gets the data packet, the data should be in the form that the attacker is unable to understand and there should be no loss of privacy whether that confidentiality is achieved by encryption or steganography or any other method. Shorly to protect the data from unauthorized access (Nobody else can access the data except the legit parties) and disclosure (The message should not be open enough). Example : Bank Account information.

★ INTEGRITY:

Integrity means to make ensure whatever the sender is sending the same message the receiver should receive. For example if a person is performing a banking transaction of 1000$. The transaction should involve only 1000$. But if the integrity is not taken care of, the attacker can modify the transaction to suppose 10000$ and also changes the destination address. So we don't want any modification in the message by the unauthorized people. And if there is any modification in the message the security system



should find that this is not the transaction initiated by the sender and should discard that message. Example : Patient's treatment from remote doctor and the doctor providing the treatment based on the data. If the data gets modifies by the attacker on the way to doctor, the patient may get wrong treatment.

★ AVAILABILITY:

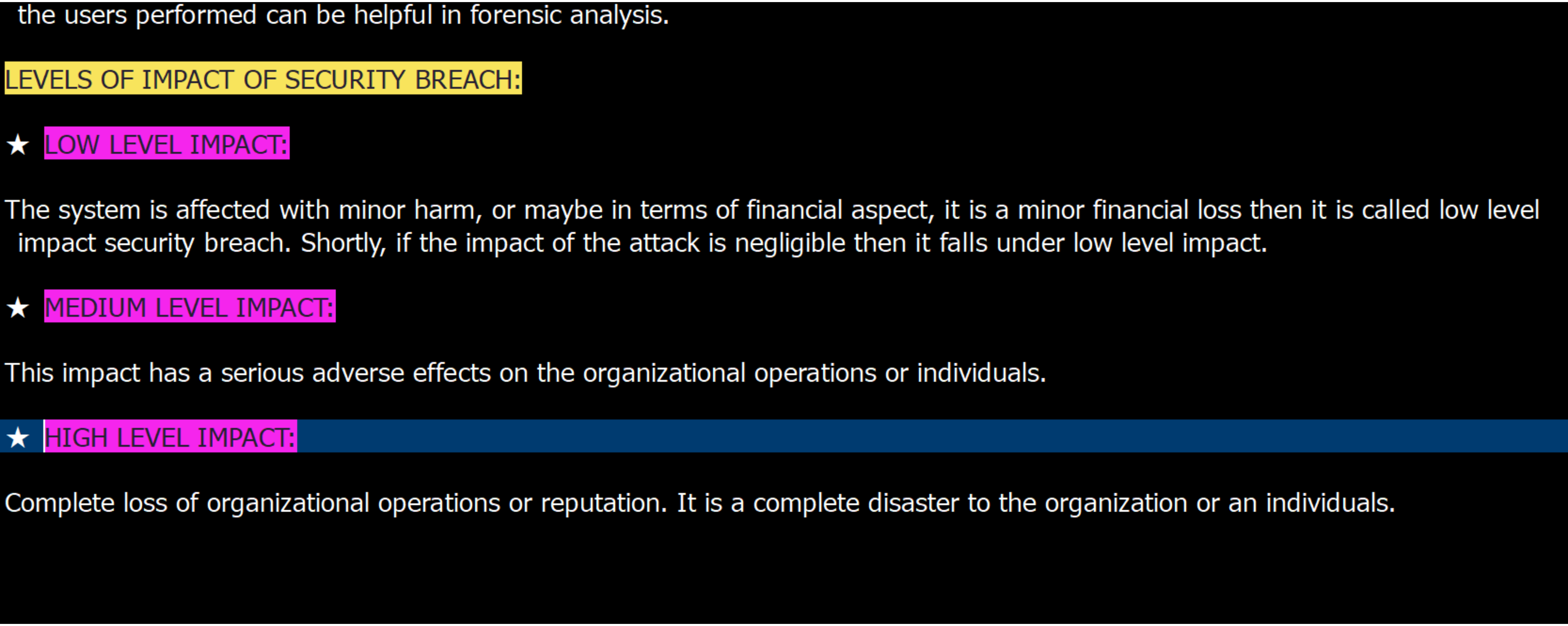
Avaliability means to ensure the timely and reliable access to the system. For example, if someone visits google now it will work, after some time if someone visits again, it will work. During this time many cyber attacks are tried on google but google still provides its services to us, means is available. Whenever any attack is launched on a server, our security system is expected to withstand those attacks and provide us service or is available despite the attacks in the same way as it was when no attack was launched on the server. This is called availablity. Example: Availability of google is a good example of availability.

★ AUTHENTICITY:

Authenticity means the property of being genuine and being able to verify the parties involved in the communication. For example: If the sender is sending some data and the receiver should be able to verify that the meassage is from the right party. Or if someone is visiting google.com, his request should get to google.com and get response from google server and not any bogus server. So the security systems should verify the parties that, are they in reality as they claim.

★ ACCOUNTABILITY:

Every individual has some privileges while working in an organization. And whatecer they perform, the system should keep record of their activities. Every user is given some responsibility and every user should have that level of privileges and the security system should ensure that the users ar not misusing their privileges. The activity is recorded, so that if any attack is launched on the organization and something feels suspicious especially related to some some insider threats, the records of the activities that



the users performed can be helpful in forensic analysis.

LEVELS OF IMPACT OF SECURITY BREACH:

★ LOW LEVEL IMPACT:

The system is affected with minor harm, or maybe in terms of financial aspect, it is a minor financial loss then it is called low level impact security breach. Shortly, if the impact of the attack is negligible then it falls under low level impact.

★ MEDIUM LEVEL IMPACT:

This impact has a serious adverse effects on the organizational operations or individuals.

★ HIGH LEVEL IMPACT:

Complete loss of organizational operations or reputation. It is a complete disaster to the organization or an individuals.