* + **Attacker vs Defender in cybersecurity**

In cybersecurity, the relationship between the role of the attacker and the role of the defender is a highly asymmetric one. While the defender must defend against all points of entry, the attacker only has to exploit one vulnerability to successfully hack into the system.

Also, defensive security is reactive in nature as only once a vulnerability is discovered can measures be taken to prevent, detect and respond to it. On the other hand, attackers seek out new vulnerabilities to exploit.

* + **What is Confidentiality, Integrity & Availability (CIA)?**

The CIA triad is a widely used model that helps guide an organization’s security efforts by aiming at fulfilling all 3 principles.

Confidentiality ensures that only authorized users and processes should be able to access or alter data. It is something that restricts access to data if the person is unauthorized. Confidentiality falls under 2 categories, authentication, and authorization. Authentication encompasses processes that allows systems to determine if a user it who they say they are e.g., passwords, authorization is about determining who has the right to access which data and just because the computer knows who you are does not mean that data access should be granted.

Integrity is about maintaining the correct state of the data and ensuring that no one can improperly modify it be it accidental or maliciously. While data integrity should be ensured by preventing unauthorized access to the data, it can be breached by ways that go beyond malicious attacked attempting to alter or delete it. E.g. any techniques designed to protect the physical integrity of storage media can also protect he virtual integrity of data.

Availability ensures that authorized users should be able to access data whenever the need to do so. Malicious attempts at disrupting availability include DDOS attacks where attacker try and overwhelm the server causing it to crash. There are also cases where availability is affected which were caused by non-malicious reasons. This includes things such as keeping hardware up-to-date, monitoring bandwidth usage etc.

* + **What is Authentication, Authorization, Auditing, Accountability?**

Authentication encompasses processes that allows systems to determine if a user it who they say they are e.g., passwords. It ensures that unauthorized personnel cannot enter the system even if they have physical access to the system as they must proof their identity.

Authorization is about determining who has the right to access which data and just because the computer knows who you are does not mean that data access should be granted. It ensures that a user must have the rights and privileges to view the data even if they work there. E.g., Workers cannot see the boss’s files even though they are registered users on the network.

Auditing is like reflecting where you take a complete review and analysis of your business’s security infrastructure, identifying vulnerabilities and exposing weaknesses and high-risk practices in the process. It helps an organization have a better understanding of their strengths and weaknesses which will allow them to take appropriate measure to secure their weaknesses and continue with their good security measures.

Accountability is about how every individual is accountable for ensuring that are not breaching any security practices and giving hackers a window to hack into the organization. It is about the consequences that an individual will face if he is careless or lacking in good security practices and about how an organization ensures that all staff members know the security practices of the or organization.

* + **Explain Non-Repudiation, Data Privacy, Data Anonymization, Personal Data Protection Act.**

Non-Repudiation is ensuring that a user cannot deny his actions that are done online. It is about having proof or evidence that signifies that a person has indeed performed an action and even if he denies it, he will be proven wrong.

Data privacy is about how a customer’s understanding on what data is being taken, how the data is being used and an overall transparency as to what the company is doing with the customers’ data.

Data anonymization is about making the data unable to point and describe a certain individual. It ensures that even if the data is breached the hackers cannot identify who the data really belongs to even if they can see the data.

The Personal Data Protection Act (PDPA) provides a baseline standard of protection for personal data in Singapore. It complements sector-specific legislative and regulatory frameworks such as the Banking Act and Insurance Act. It comprises various requirements governing the collection, use, disclosure, and care of personal data in Singapore.