The CIA Triad

The CIA Triad is a commonly used model for guiding information security policies. The foundation for this is separated in three categories: Confidentiality, Integrity and Availability. These concepts are a part of the design for policies and with this in mind, it's important to know within information security the difference between authorization and authentication.

Confidentiality, Integrity and Availability…

When looking at the CIA Triad, it's critical to be familiar with what each concept's meaning and importance within its framework. Confidentiality is similar to privacy or on a need to know basis which means protecting any sensitive information from unauthorized access. A certain example would be like organizations storing bank account information or social security. You would want to restrict access to individuals who it doesn't belong to maintain confidentiality. Integrity refers to assurance that data is true, accurate and unaltered by unauthorized individuals so that the data can be used reliably. An example would be a bank ensuring financial transactions are processed correctly and customer information is maintained in a concise way by conducting audits of transaction logs. Availability refers to information being able to be accessed by authorized personnel when they need it and some of what is involved are networks, hardware and software. An example would be a bank ensuring individuals have access to their accounts by having disaster data backups in case of an event like a fire or RAID in mainframe servers in case of disk failure so that data can be replaced immediately mantating the availability of systems. These three concepts are not separate but intertwined with each other. Together this forms the critical guide to develop policies in information security.

Authentication and Authorization…

Both authentication and authorization are similar in that they both are related to information security but have different purposes. Authentication is done before authorization. “Authentication is the process of verifying the identity of an individual”. The main way to look at how Authentication is accomplished is by something you know like passwords, something you have like a smart card or something you are, like using fingerprints.This is all done to achieve the purpose of making sure an individual is who they claim to be. “Authorization is the process of granting or denying access to specific information or service based on the authenticated individual.” An example of how this works is using the idea of an online banking system. An individual accesses their bank account by username and password or fingerprint to confirm their identity which means they have been authenticated. After this the authorization process determines what the individual is allowed to do based on the identity like for example check account balance or transfer money. Together, authentication and authorization go hand in hand to ensure that individuals are authenticated so they can access the banking system and perform actions they are authorized to do.

Conclusion…

The CIA Triad is an important part of the fundamentals of cybersecurity and helps in guiding the policies that organizations use in today's society. This concept evolved over time to become what it is now and will continue to be used because of its common use, effectiveness and proven reliability in organizations currently.

By: Adrian Galvan

Resources: https://www.onelogin.com/learn/authentication-vs-authorization
https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view