Ava McLaughlin

CYSE 200T

February 16, 2025

The CIA Triad

The Confidentiality, Integrity, and Availability (CIA) Triad is a set of guidelines for organizations to develop policies that protect their information. It serves as a common basis that guides cybersecurity practices, including authentication and authorization methods.

Confidentiality

Confidentiality refers to the protection of sensitive information from unauthorized users. When people think of Cybersecurity, they often associate it with this aspect of the Triad. Confidentiality involves creating safety measures like passwords, informing authorized users on how to protect themselves, and categorizing information based on sensitivity level (Chai, 2022). An example of confidentiality within a company is Role-Based Access Control, where employees are only granted access to the information necessary for their role. A customer service representative would likely not have access to finance documents because they have no use for them, and it would create security risks (Fortinet). Authentication and Authorization also fall under this category, which will be explained along with the differences between them.

Integrity

Integrity ensures the information presented is accurate and has not been tampered with. A breach of integrity might look like a hacker changing the grades of students at a university, or an employee changing payroll information (Duvall). It's important to protect a document's integrity because unauthorized changes can lead to misinformation, financial exploitation, or even legal issues. Integrity also includes data corruption by systems, such as a backup not saving properly or server crashes (Chai, 2022). Some remedies for Integrity breaches are digital signatures and encryption (2025).

Availability

Availability is straightforward, meaning that resources are easily accessible and work efficiently. Availability involves maintaining hardware, monitoring networks for user issues, and updating systems regularly (Chai, 2022). Availability helps users to not be prompted by other providers, and that information is accessible in a timely manner to those who need it. It also protects a company by monitoring and preventing interruptions, even during cyberattacks. It's important to have procedures in place to protect availability, such as quick server maintenance with prior notifications or a disaster recovery system (Fortinet).

Authentication and Authorization

Authentication refers to the process of identifying a user, while Authorization defines what the identified user is allowed to do. Within a company, a simple computer password may identify an employee, while an access control system specifies what resources that employee can then access (Duvall). However, authentication is an easy process to compromise, as many people have trouble managing passwords responsibly by writing them down, making them too simple, or reusing them across accounts; for this reason, methods such as two-factor authentication have been developed, which combine something you know with something you have to verify your identity (Duvall). In conclusion, the CIA (Confidentiality, Integrity, Availability) Triad serves to protect organizations from security threats by creating guidelines and methods such as authentication and authorization.

References

Chai, W. (2022, June 28*). What is the CIA Triad? Definition, Explanation, Examples*. Tech Target. https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view

CIA triad: Confidentiality, integrity, and availability. SailPoint. (2025, January 16). https://www.sailpoint.com/identity-library/cia-triad

Duvall, T. (n.d.*). CYSE-200, Mod 2C The CIA Triad and Other Cybersecurity Fundamentals*. Old Dominion University. https://docs.google.com/presentation/d/1VXWxkXVy0r7b0pfiOh1Fb0z4mWYILwt1/edit#slide=id.p

What is the CIA triad and why is it important? Fortinet. (n.d.). https://www.fortinet.com/resources/cyberglossary/cia-triad