CYSE200T Journal Entry

Write Up: The CIA Triad

Taylor Reel

Cybersecurity Essentials: The CIA Triad & Access Management

Introduction

The CIA Triad—Confidentiality, Integrity, and Availability—serves as an anchor to ensure utmost security and safety practices that promote the well-being of an organization as well as all who are affected by it; along with a solid understanding of authentication (verifying identity) and authorization (permitting access), these are the basic concepts of cybersecurity and are essential to protecting data from theft or misuse.

Confidentiality

Confidentiality within the CIA Triad is imperative, as it allows only those who are permitted and authorized to view documents and information not intended for public disclosure. One major way this is accounted for is 2-factor authentication (2FA), and now with a more advanced multi-factor authentication (MFA) ("What is the CIA Triad? Definition, Importance, & Examples," 2025). Not only is it seen on many federal sites, such as FAFSA, IRS, and NSF. This is also seen on many state-mandated sites, like the Virginia State Police Inspection Site, a website that allows Virginia state inspectors to authorize and publish valid inspection stickers required on Virginia vehicles. If this information were to be released to the public for free use, a plethora of breaches are available to compromise things as major as personal tax documents that

could result in an audit and legal recourse, or federally supplied student aid that allows students to continue their education.

Integrity

Integrity involves making sure your data is trustworthy, free from tampering, and that systems are accurate. “The integrity of your data is maintained only if the data is authentic, accurate, and reliable” (“CIA Triad,” 2025). This is a detrimental contribution to the CIA Triad, as it pertains to the access and control of data throughout its entire lifetime (Chai, 2022). Cybersecurity professionals use hashing, a way to encode sensitive data into indecipherable measures, to maintain this integrity within organizations. Tools such as digital signatures and backup systems are also examples of upholding version controls that help corporations detect unauthorized threats (“What is the CIA Triad? Definition, Importance, & Examples,” 2025). At its core, integrity is an essential part of the Triad because without reliable systems, it would be difficult to preserve trust and ensure the safety of companies.

Availability

While confidentiality and integrity are very important in this triad, they would be completely useless without the necessary availability in order to access information when needed in a prompt manner (“CIA Triad,” 2025). The concept of availability allows for necessary access to be readily available and involves making sure networks are maintained for there to be order. There would be no purpose for this information to be stored and monitored if access to it were not possible—a data void. To maintain availability, organizations tend to rely on redundant backups and monitoring performance to catch issues early on. For example, DDoS (Distributed Denial of Service) attacks overwhelm company servers when there is limited availability,

causing networks to be unavailable for legitimate users. To combat this problem, corporations use DDoS mitigation and load balancing to ensure systems are online, even during outages. Invasions are also faulted by making sure regular training is administered to staff in order to recognize and fight threats (IT Governance, 2025). Without availability, the protections of confidentiality and integrity would hold little weight, as information must remain usable to serve its purpose.

Authorization vs. Authentication

The CIA Triad closely connects with the principles of authentication and authorization. Authentication involves verifying the identity of a user or system to confirm they are who they claim to be, while authorization determines the specific access privileges granted to that authenticated identity ("Authentication Vs Authorization," 2025). The authentication process is typically done before the authorization process, and while authorization focuses more on that person's credentials and privileges, authentication focuses on who the user is. A good example of this is that any FBI employee can log onto their computer to check their email, but an employee with lower clearance is not going to have the same access as someone higher in the chain. ("Authentication Vs Authorization," 2025).

Conclusion

The CIA Triad is widely known as the three most fundamental concepts within cybersecurity. Confidentiality limits who can see what. Integrity involves making sure your data is trustworthy. Availability promotes access to authorized personnel whenever they readily need it. This triad, as well as understanding the differences in authorization and authentication, ensures the foundation of protecting data in any aspect and preventing stolen information.

Works Cited

Blog, L. C. (2025, May 22). *What is the CIA triad? definition, importance, & examples*. SecurityScorecard.com. https://securityscorecard.com/blog/what-is-the-cia-triad/

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

Fortinet.com. (2025). *What is the CIA triad and why is it important?*https://www.fortinet.com/resources/cyberglossary/cia-triad

GeeksforGeeks.org. (2025, August 28). *Authentication vs authorization*. https://www.geeksforgeeks.org/computer-networks/difference-between-authentication-and-authorization/

Governance, I. (2025, June 18). *What is the CIA triad and why is it important?*. IT Governance Blog. https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important#:~:text=Enabling%20MFA%20protects%20confidentiality%2C%20but,regulatory%20context%20of%20cyber%20risk;