The CIA Triad

Cali J. Zuk

Department of Cybersecurity, Old Dominion University

CYSE 200T

Mr. Charles Kirkpatrick

September 15th, 2024

The CIA Triad: A brief history and evaluation

Introduction

The CIA triad has its roots in military attempts to protect classified information at the dawn of the modern computing era; specifically, the Anderson Report first specified three principles of information security that now form the triad (Samonas & Coss, 2014, p. 24.) These principles are confidentiality, integrity, and availability and they are a cornerstone of modern information security practice. The CIA triad is widely used because it is simple to understand and provides broad baseline guidelines for data security (What Is the CIA Triad and Why Is It Important?, n.d.) The three principles are: confidentiality, which ensures that information is not exposed to unauthorized parties; integrity, which ensures that information is not unknowingly altered or compromised and therefore can be trusted; and availability, which ensures that IT systems are up and functional when needed.(What Is the CIA Triad_ Definition, Explanation, Examples – TechTarget.Pdf, n.d.).

Strengths and Weaknesses of the Triad

Strengths of the CIA triad include its simplicity, implementation ease, and independence of any specific framework. Indeed, all three of these aspects make the CIA triad the foundation for more complex information security frameworks and government policies such as ITIL, COBIT, and HIPAA (Samonas & Coss, 2014, p. 25). The broad scope of the CIA triad also means that the enterprise can ensure proper information security despite a lack of a more intensive governance framework. Full compliance with the three guiding principles ensures a baseline of coverage that more sophisticated frameworks can be integrated with. The ease of implementation means that even small organizations can ensure a strong security posture. In the modern era, a foundational part of the social contract between customer and business is information security, and a failure to adopt a security posture can cost the business everything.

Weaknesses of the CIA triad include its lack of specificity and its failure to include non-technical controls. The triad as taught does not include any specific tools or strategies to achieve each of its tenants. Instead it relies on the Information Security Professional to choose which tools and strategies to implement to achieve the triad. While this ensures maximum flexibility for the professional, it does leave the possibility for coverage gaps in security system design. The other main weakness is its failure to incorporate non-technical controls by default (Samonas & Coss, 2014); non-technical controls include administrative and physical controls (What Are the 3 Types of Security Controls?, 2023), and these are where the weaknesses of the triad are exposed. These other controls are essential to securing the human side of information systems and are not often thought of when professionals implement the CIA triad. Part of the issue is that they are included in the broad definition of the CIA triad, yet are seldom implemented by the practitioners devising security systems. A strong counter to this weakness is emphasizing the importance of the human factor when training cyber security professionals.

Authentication vs. Authorization

Authentication and authorization differ in that authentication verifies identity and authorization gives the user access to their assigned permissions (Kosinski, 2024). Both processes serve as key parts of an enterprise's Identity and Access Management or IAM policy (Kosinski, 2024). As an example, let's say you were invited to a friend's house for a housewarming party, when you arrive, you knock on the front door and your friend lets you in; this is authentication because your friend checked that you were invited and that you didn't bring any uninvited guests. Once inside, your friend may show you where the dining area is or the kitchen and the guest bathroom. What they would not let you see is their bedroom, their private bathroom, their kids rooms, and any other restricted area; this is authorization, as you have been given access to areas that are open to guests while certain other areas are off-limits.

Works Cited

Kosinski, M. (2024, June 28). Authentication vs. authorization: What’s the difference? IBM Blog. https://www.ibm.com/blog/authentication-vs-authorization/www.ibm.com/blog/authentication-vs-authorization

Samonas, S., & Coss, D. (2014). THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY. Journal of Information System Security, 10(3). https://www.proso.com/dl/Samonas.pdf

What are the 3 types of security controls? Explained by an expert – Cyber Insight. (2023, June 14). https://cyberinsight.co/what-are-the-3-types-of-security-controls/

What is the CIA Triad_ Definition, Explanation, Examples—TechTarget.pdf. (n.d.). Google Docs. Retrieved September 16, 2024, from https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view?usp=sharing&usp=embed_facebook