Aaron Jones

Professor Kirkpatrick

CYSE200T

9/17/2023

Write-Up: The CIA Triad

Security is an increasingly critical need for any organization, especially in the modern environment, identifiable with high data reliance and digital solutions. Specific elements of data security apply, including the preoccupation with handling complex and large data, striving for efficiency, and constantly responding to the changing technological landscape. The use of data in decision-making also leads to greater attention to its reliability, access, and security. It makes organizations invest heavily to achieve the desired outcomes and digital positions. The CIA Triad is a critical model for developing and actualizing a security protocol and system. The model exists beyond the current systems by intervening in common concerns, beginning with establishing vulnerabilities (Bhattacharjya 405). There cannot be a perfect system, yet it is often difficult to define the foundations for threats and establish lasting solutions. The CIA Triad also defines an ideal solution so that an organization can seamlessly exploit its technological systems. Additional provisions apply, including regulatory compliance and business continuity.

Elements of the CIA Triad

The CIA Triad is a strategic model designed to cover universal security elements for any organization. It covers three fundamental components, including confidentiality, integrity, and availability. Confidentiality entails ensuring adherence to the users' need for privacy and autonomy. It is also a foundation for providing safeguards for sensitive information (Chai 1). Every set of data is bound to have predefined levels of authority and ownership. Therefore, it is

imperative to inhibit unauthorized access, which can be based on internal and external users. Integrity is also an important element of the CIA Triad and is relevant to every security system's inclination for optimal security and value. File permissions are some of the immediate elements of integrity regarding a security system. It means that a system ought to anticipate that the users and owners of data desire security and permission to define who should access or use their resources. Lack of permissions suggests overlooking the need for honesty, an important value in business and information management.

Integrity also leads to observing user access controls, which need to be effective and seamless for the benefit of all users of information. Availability is the third component of the CIA Triad, also providing important incentives for the handling of data for individuals and organizations. It refers to the active nature of the CIA Triad, where professionals and protocols apply toward achieving desired security and efficiency standards. Hardware maintenance and repairs are some of the vital aspects of availability under the triad (Chai 2). It is imperative to consider specific precautions and improvements whenever a risk occurs. Ultimately, an organization can achieve the desired functionality of its operating systems based on a series of precautions and interventions. While every element of the triad provides critical incentives to the organization, specific incentives offer greater benefits. Confidentiality emerges as a critical element, especially considering the availability of technical instruments to promote availability and integrity. Data users are increasingly interested in the assurance that their details remain safe and private.

Differentiating Authentication and Authorization

Authentication and authorization are also essential tenets of the CIA Triad, the achievement of an ideal digital security environment. Each term represents a central requirement

for optimal security and exists interchangeably, yet there are unique differences between each. The order in which each element occurs is one of the immediate contrasting elements. Authentication occurs first with specific immediate provisions of a security system, including parties with access rights and the means of determining the suitability of a user. Authorization follows based on predefined specifications and precautions for every user (Yee and Mohamad Zolkipli 36). Also, the authorized person might have limited or full access to a system and consider specific actions. The meaning of each process also provides in-depth differences between the two elements of the CIA Triad. Authentication covers the series of actions, processes, and tools for verification of a user's identity. However, authorization denotes specific privileges to a given use based on anticipated importance or precaution. Authentication comes in handy while verifying the kind of access made to a database. It considers unusual behaviors and conditions. Conversely, authorization can often define the kind of access that can be availed based on applications, files, or categories of information.

Example

An example involving the CIA Triad in an organizational context involves the management information system used in the finance department. While the department has different employees with similar roles, there are predefined levels of authority and access to information. The departmental manager will often have maximum capacity, including accessing every file and every other employee's system. However, the subordinates will often have limited access and would not edit essential information without the authorization of the management. Also, in the event of loss or breach of privacy or corruption of details/files, it would be possible to link the issue to a given person.

Summary and Conclusion

Essential elements of data security revolve around handling complex and large data, striving for efficiency, and constantly responding to the changing technological landscape. The CIA Triad also defines an ideal solution so that an organization can seamlessly exploit its technological systems. The model is a strategic model designed to cover universal security elements for any organization. It covers three fundamental components, including confidentiality, integrity, and availability. Confidentiality entails ensuring adherence to the users' need for privacy and autonomy. Integrity is also an important element of the CIA Triad, and it is relevant to every security system's inclination for optimal security and value. Integrity also leads to observing user access controls, which need to be effective and seamless for the benefit of all users of information.

Works Cited

Bhattacharjya, Aniruddha. "A holistic study on the use of blockchain technology in CPS and IoT architectures maintaining the CIA triad in data communication." *International Journal of Applied Mathematics and Computer Science* 32.3, 2022. vol. 32, no. 3, 403–413. https://www.researchgate.net/profile/Aniruddha-Bhattacharjya/publication/365891730_A_Holistic_Study_on_the_Use_of_Blockchain_Technology_in_CPS_and_IoT_Architectures_Maintaining_the_CIA_Triad_in_Data_Communication/links/63885e07148d2362a4b6491e/A-Holistic-Study-on-the-Use-of-Blockchain-Technology-in-CPS-and-IoT-Architectures-Maintaining-the-CIA-Triad-in-Data-Communication.pdf

Chai, Wesley. What is the CIA Triad? Definition, Explanation, Examples, 2022. https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view

Yee, Chai Kar, and Mohamad Fadli Zolkipli. "Review on confidentiality, integrity and availability in information security." *Journal of Information and Communication Technology in Education* 8.2 (2021): 34-42. https://doi.org/10.37134/jictie.vol8.2.4.2021