The Confidentiality, Integrity, and Availability (CIA) Triad

My Nguyen

Old Dominion University

CYSE200T

Professor Kirkpatrick

April 18, 2024

The Confidentiality, Integrity, and Availability (CIA) Triad

Cybersecurity in the social, corporate, business, and political world of technology is an essential pillar that cannot be dispensed. The CIA triad acronym represents three tacit ideologies that bridge good relations in almost all sects of life. With its itinerary and rapid technological advancements, cybersecurity forms the epicenter, brokering success and enchaining realms that endanger data ranging from individual to organizational security. However, as technology advances, cyber security and data breaches continue to rise (Desmedt & Boot, 2022). This discussion enchants the inarguable relevance of the CIA triad practical application in pursuit of a secure and digital environment for socioeconomic and political thrive achieved through an exhaustive examination of the triad pillars.

The pillars of the CIA Triad

(1) Confidentiality

Confidentiality ensures that information is directed and consumed by the intended person without traversing through unauthorized hands or disclosure. This pillar plays a big role in minimizing the ransomware attacks individuals and organizations face. According to Data Protection Trends Reports conducted by Veeam in 2024, about 75 percent of organizations in 2023 suffered from ransomware attacks affecting and endangering some of their vital operations. This contention implies that information meant to be contained within organizational bounds leaked into the wrong hands and got used to appropriate theft, attracting losses (Moller, 2023). This pillar ensures the accessibility of information to authorized entities through reliance on methods such as encryption and access control.

Encryption is a confidentiality strategy in which messages are substituted from the holistic letters readable by mass to particular numbers that can only be decoded by authorized

persons. Unauthorized individuals cannot access such information due to the use of encryption methods. Access control serves as another method to safeguard the confidentiality of information (Khandare et al., 2023). This digital gatekeeper processes authentications and permissions to retrieve specific data. An access control strategy installation prevents cyber security perpetrators from accessing information due to a lack of authentication user guides.

Nonetheless, technological advancements still expose individuals and organizations to the stern danger of cyber manipulators who craft ways of accessing and tampering with the confidentiality of such protected information. As a result, organizations have developed strategies like the zero-trust policy, which advocates for strict adherence to stringent guidelines and principles that facilitate the authentication of IT applications, devices, and users. Some of the zero policy measures to harness the confidentiality of information include explicit verification, assumed breach, and least privilege access (Desmedt & Boot, 2022). The three mechanisms boost adherence to guidelines and principles for information access, aiding compromise of any kind that information users could initiate.

(2) Integrity

In its precepts, integrity in cybersecurity is the ascertainment of the accuracy and consistency of data throughout its entire lifecycle. Enforcement of integrity thus assures that information is channeled to the intended party without alterations or temperance. Socially manipulating data or any form of corruption with data exposes it to the dangers of decision flaws, which can lead to misguidance. A business breach of data integrity deciphers consistency and accuracy, eventually leading to poor business decisions and losses (Moller, 2023). It is, therefore, vital to protect the integrity of information using tools and practices like checksums and version control. Checksum integrity control is a digital appliance that takes individuals'

fingerprints with prior permission to access information within an organization or sole proprietorship firm. This gadget detects and examines the configuration of fingers in the registered print of authorized personnel for access to such information (Pawar & Palivela, 2023). Suppose there needs to be more configuration of the current finger than the previous finger used to access information. The instrument sends signals to reject access until authorized fingers are placed.

On the other hand, version control preserves information integrity by keeping track of documents or files prepared and registered with the machine. This suggests that the machine can only restore previously registered versions of documents or files. Version control upholds the dignity of information by preventing additional documents from finding their way to the one previously stored in the machine's memory. While maintaining integrity is costly due to various installations and monitoring, it prevents cyberattack forgery information from remaining accurate and reliable and allows users to use it in decision-making (Khandare et al., 2023). Integrity also paves the way for business growth due to the optimal monitoring of processes through protective methods. However, this does not prevent cyberbullies from acting in bad faith and exposing control tools to manipulators. Individuals pursuing information integrity should thus invest in technology to bring their security tools to the latest sophistication that can reduce cyber insecurity.

(3) Availability

In the context of cybersecurity, availability refers to the accessibility of information and resources by particular individuals at a time when they need them. Enhancing information availability enables the growth and continuity of organizations and promotes operational efficiency. The availability of required information still protects and minimizes possible

downtime situations that may adversely impact actual and potential productivity (Desmedt & Boot, 2022). For social groups, the inability to access essential information is at the forefront of failures that thwart trust and solidarity. Businesses are no exception; a lack of adequate access to relevant information can cause losses, especially if such information contains major precepts and decisions controlling business operations. Strategies to enhance information access include backup solutions and redundancy plans. A backup solution is the application of data safety nets that enable organizations to restore data by backing it up in case of undesirable events like system failure, cyberattacks, and other unpredictable disruptions (Pawar & Palivela, 2023). These safety nets also facilitate business or organization continuity by easing the storage and retrieval of important information useful on rare but essential occasions.

By developing duplicate alternative systems, redundancy plans improve cybersecurity by easing access to information. This tool ensures that one system's breakdown or malfunction continues the organization's entire operation. The redundancy plan also allows for uninterrupted access to data propagated by the main data system in the event of a failure. Organizations never expect data loss, but data availability is tested in real-life scenarios during crises (Sadik et al., 2020). Organizations with well-developed availability plans can withstand disaster tides and remain resilient at critical moments. Disruptions throw organizations off balance without properly developing plans for accessing relevant data and may end up closing.

In summary**,** social and financial institutions must play safe from cybersecurity. The realization of cyber-secure metrics brings about sanity and enhances the growth of individual and institutional entities. Regarding our case, each confidence, integrity, and availability (CIA) pillar plays a significant role in surfacing the security and trustworthiness of the digital business and social operating environment. The comprehension and implementation of the discussed CIA

nuances secure individuals and other entities from losing vital information assets while enabling them to boost their trust with clients and associate stakeholders. Companies of all sizes use the CIA Triad principles in everyday business. However, integration of these principles varies depending on the nature and scope of political and business backgrounds (Pawar & Palivela, 2023). For service providers, CIA principles enable them to deliver services on time and with utility autonomy. Other platforms, like e-commerce businesses, also rely on confidence, integrity, and availability strategies to preserve data on transactions that help them manage their market.

Organizations should, therefore, employ esteemed reliance on CIA triad nuances to enhance cybersecurity and remain functionally free from unnecessary cyber disruptions and attacks, regardless of size. Nonetheless, the discussed metrics are not the only ways to restore safety to businesses due to rapidly growing technology, with cyberbullies inventing sophisticated strategies to attack (Sadik et al., 2020). Individuals and organizations should keep an eye on the upcoming digitalization to provide better and more solid measures for curbing the cyber-insecurity menace.

References

Desmedt, L., & Boot, F. (2022). Information security for Industry 4.0. https://arno.uvt.nl/show.cgi?fid=159549

Khandare, S. V., Herlekar, V. P., Hanwate, V. S., Shirale, G. M., & Sirbhate, D. D. (2023, February). A Global Overview of Data Security, Safety, Corporate Data Privacy, and Data Protection. In *International Conference on Intelligent Computing and Networking* (pp. 437-451). Singapore: Springer Nature Singapore. https://link.springer.com/chapter/10.1007/978-981-99-3177-4_32v

Möller, D. P. (2023). Cybersecurity in digital transformation. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 1-70). Cham: Springer Nature Switzerland. https://link.springer.com/chapter/10.1007/978-3-031-26845-8_1

Pawar, S. A., & Palivela, H. (2023). Importance of least cybersecurity controls for Small and Medium Enterprises (SMEs) for better global Digitalised economy. In *Smart Analytics, Artificial Intelligence and Sustainable Performance Management in a Global Digitalised Economy* (pp. 21-53). Emerald Publishing Limited. https://www.emerald.com/insight/content/doi/10.1108/S1569-37592023000110B002/full/html

Sadik, S., Ahmed, M., Sikos, L. F., & Islam, A. N. (2020). Toward a sustainable cybersecurity ecosystem. *Computers*, *9*(3), 74. https://www.mdpi.com/2073-431X/9/3/74