CIA Triad: Fundamentals and Issues

Leyah Knox

The CIA (Confidentiality, Integrity, Availability) triad is a fundamental conceptual tool within the field of cybersecurity to ensure that information and computer systems remain secure. The three elements of the triad interact with each other to provide assurance that information is not only confidential, but also reliable, and accessible when required. As described by TechTarget, confidentiality defines who has permission to view information, integrity ensures that information remains reliable and trustworthy, and availability ensures that authorized personnel can access information when necessary. The significance of the CIA triad lies in the fact that cybersecurity is not solely concerned with preventing unauthorized access to information. Cybersecurity is equally concerned with ensuring that information is accurate, and that systems operate as intended. Failure to adequately protect any component of the CIA triad can result in significant problems for both individuals and organizations. Confidentiality refers to the ability to restrict unauthorized viewing of information. In my opinion, confidentiality is the act of preventing unauthorized individuals from accessing confidential information. Examples of confidential information include Social Security numbers, passwords, medical records, financial information, and proprietary business information. Confidentiality is significant due to the potential consequences associated with loss of confidentiality including identity theft, financial hardship, privacy violations, and harm to an organization's reputation. Examples of measures that organizations may implement to safeguard confidentiality include strong passwords, access control mechanisms, encryption technologies, and multi-factor authentication. Training employees on methods to identify phishing schemes and other forms of social engineering is another critical measure to protect confidential information. Integrity refers to the ability to

ensure that information remains accurate and reliable. In my opinion, integrity refers to the ability to verify that information has not been altered, deleted, or manipulated by an unauthorized individual. Similar to loss of confidentiality, loss of integrity can lead to similar negative outcomes.

For instance, if an unauthorized individual modified an individual's financial or medical records, an individual could make critical decisions based upon inaccurate information. Measures that organizations can utilize to protect integrity include access control mechanisms, file permission settings, security logging, checksums, digital signatures, and backup systems. Utilizing these security measures can assist organizations in identifying unauthorized modifications to information and restoring information should an incident occur. Availability refers to the ability to ensure that authorized users have access to information and systems when required. In my opinion, availability refers to the ability to maintain continuous operation of systems to allow users to utilize them rather than experience downtime resulting from an attack or technical malfunction. Availability is particularly significant for organizations whose daily operations rely heavily on technology. For example, if a hospital's computer systems cease functioning, hospital staff members may be unable to retrieve essential patient information. Conversely, if an organization's systems become non-functional, customers may be unable to complete purchases and employees may be unable to perform their job duties. Examples of measures that organizations can employ to enhance availability include conducting routine maintenance activities, applying software updates promptly, implementing redundant systems (backup systems), monitoring network traffic, and developing disaster recovery plans. An example illustrating a failure of confidentiality is the 2017 Equifax data breach. Equifax was one of the largest credit reporting agencies that collects vast quantities of personal information

regarding consumers. According to reports issued by the U.S. Government Accountability Office (GAO), hackers accessed Equifax's systems via an online dispute resolution platform and subsequently obtained personal information pertaining to approximately 145.5 million individuals. The personal information included consumer name, address, date of birth, Social Security number and other confidential information (GAO, 2018). Subsequent reports issued by the Federal Trade Commission (FTC) indicated that approximately 147 million consumers were affected by the breach. The compromised data can be utilized by perpetrators of identity theft and fraud. The Equifax breach demonstrates why confidentiality is so essential. The primary problem was that hackers were able to gain unauthorized access to confidential customer information. Further exacerbating the problem was that Equifax exhibited numerous vulnerabilities in its security posture.

Notably among these vulnerabilities was that Equifax neglected to apply a patch for a known software vulnerability. Other vulnerabilities included deficiencies in network security and protection of login credentials. According to reports issued by the FTC, Equifax had been advised of a severe vulnerability but failed to ensure that the system was adequately patched. Once the hackers gained initial entry into Equifax's systems, they were capable of navigating through Equifax's network and extracting additional information. Beyond Equifax, the ramifications of the breach extended to millions of individuals who experienced increased risk of identity theft and fraud due to exposure of their Social Security numbers, dates of birth and other personal data. Many individuals spent considerable time reviewing their credit reports and implementing protective measures to mitigate risks associated with loss of identity.

Additionally, Equifax endured financial losses and reputational damage. In 2019, Equifax agreed to remit payments totaling at least $575 million in conjunction with a settlement agreement reached with the FTC, Consumer Financial Protection Bureau and various state/territory attorney general offices. Pursuant to the terms of the settlement agreement, Equifax was also required to enhance its information security protocols. Collectively, this illustrates how cybersecurity incidents can negatively impact customers, financials, public confidence and an organization's reputation. Organizations can implement several strategies to reduce likelihood of future breaches akin to Equifax. First, organizations should regularly assess their systems for vulnerabilities and apply necessary software updates as soon as feasible. Second, implementing network segmentation and least-privilege access can limit scope of access available to an attacker should they successfully penetrate a single system within an organization's network. Third, organizations should establish robust authentication mechanisms and access controls to safeguard passwords and other login credentials. Fourth, organizations should monitor their systems continuously to facilitate prompt detection of anomalies indicative of suspicious activity. Lastly, organizations should create backup systems and contingency plans to recover systems should they fail as a result of an attack. Implementing these practices will support protection of all three components of the CIA triad by preserving confidentiality (privacy) of information, integrity (accuracy/reliability) of information, and availability (accessibility) of information. TechTarget additionally recommends establishing access controls, encryption, two-factor authentication for confidentiality, logging, checksums, backup systems for integrity, and monitoring systems, system updates, backup systems, recovery plans for availability.

In conclusion, the CIA triad serves as an effective model for understanding cybersecurity because confidentiality, integrity, and availability function collaboratively. Confidentiality preserves confidentiality (privacy) of information, integrity preserves reliability/accuracy of information, availability enables users to access systems when needed. The Equifax breach represents a classic illustration of adverse consequences that can arise when fundamental security practices are disregarded. Cybersecurity encompasses more than technological components, organizations must also provide employees with training on identifying/avoiding scams/phishing schemes, develop sound security policies, monitor systems for suspicious activity, create contingency plans for recovering systems following attacks. Adhering to principles embodied within the CIA triad can aid organizations in safeguarding sensitive information, and maintaining operational continuity of systems, preserving trust relationships with customers.

1. Liu, Che-Wei, et al. “Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions.” *Journal of Management Information Systems* [Abingdon], vol. 37, no. 3, July 2020, pp. 758–87, https://doi.org/10.1080/07421222.2020.1790190.

2. Shaikh, Faheem Ahmed, and Mikko Siponen. “Information Security Risk Assessments Following Cybersecurity Breaches: The Mediating Role of Top Management Attention to Cybersecurity.” *Computers & Security*, vol. 124, no. 102974, January 2023, https://doi.org/10.1016/j.cose.2022.102974.