**Understanding the CIA Triad Model: Ethical and Political Standpoints**

Kerby Guillaume

CYSE 200T

6.27.2025

*In this paper, I discuss the CIA Triad and the philosophical standpoints of this model. This analysis will examine what the* ***CIA Triad is, cybersecurity related benefits that come with CIA, ethical standpoints, and the long term ramifications of the model****; demonstrating possible changes necessary to produce a more effective framework beyond technological aspects. Understanding this model is critical to a cybersecurity analyst because it provides specific points of interest and principles to serve as guidelines when it comes to evaluating risks, designing safeguards, and responding effectively to threats.*

**1.0 Framework Core: The NICE Framework**

Before we dive in, let’s initially understand the use of models and framework in cybersecurity. In earlier modules, we were introduced to the **NICE Framework** which is **used to improve critical cybersecurity infrastructure**; a great example of how this framework structure is executed. The framework was developed to establish organized structure within the cybersecurity workplace. These help associates within the organization with their operation tasks in order to produce overall efficiency. The framework is broken down to different categories which emphasize certain points of interest regarding cybersecurity (*most framework models are usually broken down in subcategories that focus on specific points)*.

**1.1 Framework Categories: Work Roles**

One of these categories would be the specific work roles of the associates. The roles include communication security management, cybersecurity planning, workforce management, curriculum development, instruction, legal advice, leadership, privacy compliance, product support management, program management, control assessment, system authorization, systems security management, technology portfolio management, and lastly, program auditing. The work roles are designed to provide leadership, management, direction, and advocacy so the organization may effectively manage cybersecurity-related risks to the enterprise and conduct cybersecurity work.

**2.0 The CIA Triad Model**

The CIA Triad has similar structure to the framework core described, adding emphasis to three specific elements in cybersecurity: **confidentiality, integrity, and availability**. All three of these elements are essential in the security of information systems. Here are elements of CIA broken into detail:

**2.1 Confidentiality**

When dealing with information security, privacy and protection is always the top priority. **Confidentiality** involves **protecting sensitive information from unauthorized access**, ensuring that only individuals with the appropriate permissions can view or use the data [1]. The first step in making sure data is secure is to determine who is authorized to access data information in addition to being able to recognize those who are authorized (Chai 2022). In some cases private information can be accessed inevitably. Efficient ways to combat these incidents are by implementing multi-factor authentication as well as maintaining trained personnel that are aware of possible threats and ways to avoid such dangers [2]. With an established method of data protection, information security can be secured in the right hands which prevents attacks and/or loss of data (Chai 2022).

**2.2 Integrity**

**Integrity** refers to the accuracy and consistency of data—**all information stored in an organization must be true to itself** as its integrity is what helps the business succeed [1]. Network data cannot be altered in unauthorized or undetected ways and to prevent this from happening, tools such as audit logs are implemented (Fortinet 2025).

**2.3 Availability**

**Availability** ensures that information and systems are accessible to authorized users whenever needed. **There’s no business without data being present.** In order for data to be present, the systems functioning behind the scenes must perform at their best [1]. In addition, an organization can improve the availability of its data by upgrading their software systems, allowing data to become more efficient to its consumers (Chai 2022). This involves strategies such as **regular maintenance, backups, and defenses against distributed denial-of-service (DDoS) attacks** [2]—which leads me to my next point.

The risks within the cyber technology universe are quite known to all as well as the importance of protection amongst outer networks. Major breaches with malicious intentions are described as **“attack on availability.”** This title is associated with cyber attacks because this form of hacking shuts down access to the network systems so users cannot use them [3]. Now there are many kinds of attack on availability incidents but one of most common forms are DDoS.

**3.0 Attacks on Availability: Distributed Denial of Service**

We have an understanding of different strategies used in the CIA Triad but it is also important to understand the type of risks these networks could fall victim to in addition to how often these risks can occur. A major example of this type of risks are **distributed denial of service attacks (DDoS)** which can impact the element of availability in relation to the CIA Triad. A distributed denial of service attack is exactly what it sounds like. While no physical data is manipulated in these attacks, **hackers manipulate various networks, usually targeted networks**, in order to deny access to its original user [1]. This is actually done by overwhelming the system. The memory is hijacked to overload until it eventually crashes. When this happens, the CPU denies access to any websites, software applications, or even access to the network itself.

**4.0 The CIA Triad: Long Term Political Understanding**

Examining the CIA Triad,—Confidentiality, Integrity, and Availability, we can conclude that this framework is surely effective in cybersecurity and the protection of information systems, however we must ask ourselves ***“how much longer can we depend on this model?”*** Over the long term, relying only on the triad could create problems if it doesn’t grow to **address new ethical, political, and social issues.** The model is great for protecting systems and data, but it doesn’t cover political issues [1]. For example, governments or companies might justify mass data collection in the name of confidentiality, but that can violate people’s privacy if not done transparently (Greenleaf, 2019). Integrity focuses on data being correct, but it doesn’t deal with the rise of fake media, which can spread widely without altering any files (West, 2018). And while availability is important, it can lead to unethical control of services, which makes some systems more vulnerable to attack or harder for everyone to access equally (De Filippi & Hassan, 2016) [2]. To address this, we must expand the CIA Triad to include ethical and societal values. Updating policies regularly, **involving the public in decisions** can help make sure cybersecurity continues to protect both systems and society as a whole [3].

**4.1 The CIA Triad: Ethical Understanding**

When considering the CIA Triad from an ethical standpoint, we recognize that there are specific changes that would be necessary to improve the implementation of the model. While the triad effectively addresses core technical principles, it does not account for concerns such as ethical use of data. These issues matter because cybersecurity affects real people. **The biggest change would be a shift in focus to direct the importance of confidentiality, integrity, and availability beyond just technological aspects—emphasizing ethical standpoints such as accountability and transparency** [1]**.** The cybersecurity strategies in confidentiality can be implemented in societal aspects in the government; maintaining that confidentiality in order to prevent invasion of privacy in any way. Integrity policies should extend beyond technical accuracy to include ethical obligations to prevent misinformation and ensure fair decision-making. Similar to the concept in accordance with the triad, availability must be safeguarded in order to be efficient in its use to promote and contribute to societal ethical values [2].

**Conclusion**

To summarize all the points that have been stated, the CIA Triad: *Confidentiality, Integrity, and Availability*, remains an effective model in cybersecurity, offering the essential guidance for protecting data and information systems. As this paper has shown, each element of the triad plays a crucial role in digital environments through access control, data accuracy, and system reliability. However, while the triad is effective at addressing technical concerns, it falls short in recognizing the ethical, political, and societal challenges that are relevant in today’s world. Additionally, concerns such as data privacy, misinformation, and unequal access to digital infrastructure reveal the need for a more diverse framework. Moving forward, cybersecurity policies must evolve to go beyond the traditional CIA Triad by incorporating values like accountability and transparency. By doing so, we can ensure that cybersecurity not only protects systems, but also upholds ethical standards and serves the needs of society.

**Works Cited**

*Chai, Wesley. “What Is the CIA Triad? Definition, Explanation, Examples.” 2022.*

*De Filippi, P., & Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code. First Monday.* [*https://doi.org/10.5210/fm.v21i12.7113*](https://doi.org/10.5210/fm.v21i12.7113)

*European Union Agency for Cybersecurity (ENISA). (2021). Ethics and cybersecurity: Challenges and recommendations.* [*https://www.enisa.europa.eu/publications/ethics-and-cybersecurity*](https://www.enisa.europa.eu/publications/ethics-and-cybersecurity)

*Greenleaf, G. (2019). Global Data Privacy Laws 2019: 132 National Laws and Many Bills. Privacy Laws & Business International Report.
West, D. M. (2018). How to combat fake news and disinformation. Brookings Institution. https://www.brookings.edu/articles/how-to-combat-fake-news-and-disinformation/*