Mackenzie Cooke
02/02/2025

CYSE 200T 25962
Mr. Kirkpatrick

# The CIA Triad

*Confidentiality, integrity, and availability are components of a triad that provides guidelines and best practices within cybersecurity. Authentication is verifying who a user is, and authorization is deciding what they have access to. An example of authentication is the password to an account, while an example of authorization would be share drive permissions within a network.*

## What is the CIA Triad?

The CIA triad stands for confidentiality, integrity, and availability (Hashemi, 2022, p.1). It is a model used for policies within information security that covers the basis of cybersecurity protection. Without a leg in this triangle, the information that is supposed to be protected can be a significant risk. Cybersecurity professionals use this model as a guide to creating rules and best practices within the industry (Hashemi, 2022, p. 2). The CIA triad is a valuable tool used by many professionals.

## Confidentiality

Confidentiality ensures that only those with permission to sensitive or specific data have access. Cybersecurity professionals use confidentiality to protect sensitive information from unauthorized personnel who do not have the proper authorization. Different strategies to ensure confidentiality include access controls, encryption technologies, and data classification (Cochran, 2024, p. 5). Access controls allow only specific people to have keys to particular information (Cochran, 2024, p. 5). Encryption makes data unreadable by humans without the proper way to

"unlock" the information (Cochran, 2024, p. 5). Data classification allows information to be protected according to classification, ensuring more sensitive data is protected (Cochran, 2024, p. 5).

## Integrity

Data integrity is like a stamp of approval that no unauthorized access has occurred within a document. Without it, no one could trust the authenticity of the data within the file (Cochran, 2024, p. 7). Data can maintain integrity through hash functions, digital signatures, and version control (Cochran, 2024, p. 8). A hash function is a unique marker for data that will not change unless it has been tampered with (Cochran, 2024, p.8). Another way of verifying data integrity is through digital signatures, essentially just the digital version of a physical signature on an official document (Cochran, 2024, p. 8). Version control is another way to verify the data integrity and record changes (Cochran, 2024, p. 8).

## Availability

Availability prevents data loss and keeps networks and systems current (Hashemi, 2022, p. 6). It's the third component of the CIA triad, essential in maintaining data protection security, just like the others. "Availability through uptime management, service level agreements (SLAs), and redundancy and backup strategies" (Cochran, 2024, p. 12). Minimizing downtime allows data to be available to authorized users, and service level agreements are rules by which authorized users agree to abide for a safe experience (Cochran, 2024, p. 12). Lastly, redundancy

and backups ensure smooth use of systems and reliable copies of data in case of system failures (Cochran, 2024, p. 12).

## Authentication & Authorization

Both authentication and authorization are essential within the CIA triad and cybersecurity practices. Authentication is a process that systems use to verify that it is you (Leslie, 2010, p. 4). Examples of authentication include passwords and security questions. Authorization occurs after they know it's you but are now trying to determine what you can do (Leslie, 2010, p. 5). Authorization can be specific user roles within a network, like share drive access. Both authentication and authorization bring another layer of security to information systems and sensitive data.

## Conclusion

The CIA triad includes confidentiality, integrity, and availability (Hashemi, 2022, p.1). Confidentiality is the key to a system or network allowing information access, and integrity is the assurance that unauthorized users haven’t changed information (Cochran, 2024, p. 5). Availability ensures access to sensitive data, and the system updates regularly (Cochran, 2024, p. 12). Authentication guarantees a user's identity (Leslie, 2010, p. 4). Authorization ensures what an authenticated user can and cannot do (Leslie, 2010, p. 5). All of these make up the baseline for cybersecurity within systems and businesses.

**References**

Cochran, K. A. (2024). *Cybersecurity Essentials: Practical Tools for Today's Digital Defenders*. Apress.

Hashemi, C. (2022). *What is the CIA Triad? | Definition from*. TechTarget. Retrieved February 2, 2025, from https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Leslie, E. (2010). Authentication vs Authorization. *Multichannel News*, *31*(8), 22-.