

## Write-Up: The CIA Triad

Using the Chai Article, along with additional research you will conduct on your own, describe the CIA Triad, and the differences between Authentication & Authorization, including an example.

The CIA triad is not what most people think of when seeing those letters. In terms of cybersecurity, the CIA triad stands for “Confidentiality, Integrity, and Availability”. In summary, the triad is a set of concepts that are “best practices” that organizations can follow regarding their data in order to best protect it, keep its integrity, and keep it available.

When it comes to “Confidentiality”, the main thing here is protecting an organization’s data from unauthorized access and potential attackers. Protecting the information involves encryption, access control, and making sure strong passwords and 2FA/MFA are in place. With the rise in cyber attacks in recent years, it is more important than ever for organizations to focus on the “C” within the CIA Triad.

Next in the triad is “Integrity”. This part of the triad is going to make sure that the data is accurate and has not been altered in any way. It should always be consistent, and regular tests should be run to make sure it has not been modified in any way. There are a number of ways that this can be done; using correct file permissions, cryptographic checksums on files, and version control systems. The use of digital signatures to verify certain software is legitimate and that any updates have not altered it.

The last part of the triad is “A” which stands for Availability. This is going to cover the uptime of services and websites as well as making sure that authorized users can access the information and networks when they need to. This is imperative to making sure a prompt

response is taken when security incidents or data breaches occur. Availability is very important when it comes to recovery plans. Regular backups must be automatically made and stored properly. Servers should be configured with strong firewalls, and any cloud storage should be with a reputable company that has a proven history of being reliable.

Some similar concepts to the three that make up the CIA Triad are authentication and authorization. These two concepts are similar but have some key differences. Authentication is the practice of verifying the user is in fact who they claim to be. This is done by verification using a password, token, or biometrics such as a fingerprint or retina verification. Authorization comes after authentication and is used to determine what the user is allowed to access and what functions they have within a specific part of a network or system.

A good example of authentication and authorization is shown when an employee logs into their system and has to enter their credentials and also verify using 2-FA to authenticate their identity. After they have successfully logged in, they can then access things like their emails, private data and files, company records, and more. The access given to each employee is determined by the system administrator who then reports to executive management.

## Reference

Chai, W. (2022, June 28). What is the CIA Triad? Definition, Explanation, Examples.

TechTarget. <https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA>