

Name: Charles W. Pridgen

Date: February 2nd, 2024

The CIA Triad

Confidentiality, Integrity, and Availability, (The CIA Triad) are the three most core elements cybersecurity needs to be effective, as well as an organization's guide for creating information security policies. This writing will begin by breaking down each part of the triad, followed by what the triad is as a whole. Finally, we will explain the difference between authentication and authorization, and provide an example.

Confidentiality

In the article wrote by Wesley Chai called “What is the CIA Triad? Definition, Explanation, Examples,” Wesley compares confidentiality to privacy. Companies collect sensitive data/information they need to keep secret, whether it's a project to gain an edge on competitors, or personal information on customers. Everyone does not need to know everything about the company or the data that is collected, so companies assign information to different categories, limiting it to only people who have the “need to know” to perform their job. Specific training is often given to help personnel develop safe practices to guard sensitive data, as well as highlight different tactics hackers might use to access the information or take advantage of unsuspecting victims, tactics like phishing and pretexting.

Integrity

Integrity refers to keeping data trustworthy, accurate and consistent over its entire lifecycle. When you access important data, can you be sure it wasn't tampered with and is accurate? Steps are put into place to ensure the integrity/reliability of data, is not altered or lost when being accessed.

Availability

Data must be readily available when needed by authorized personnel to carry out their duties. Networks should be constantly monitored and by maintaining critical hardware, upkeeping the facilities they are stored in, and having a plan to fully recover any lost data, cybersecurity personnel can readily provide data in the event of hardware failure, human error, natural disaster, etc. Wesley Chai stated, "Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important tactics." All these things will help keep the flow of data/information effectively.

The CIA Triad

When these three elements are viewed together as one model, (CIA Triad) organizations can use it as a guide in building effective cybersecurity policies and measures. Integrity of data is key, but without confidentiality, that integrity can be compromised. Someone with access to sensitive information who loses confidentiality, exposes sensitive data to third party attack, degrading data integrity, which could affect the availability of data as well. Organizations maintain confidentiality by training personnel to identify social engineering, mitigating threats that could steal and exploit the data they have access to. Assisting in developing safe handling of critical data, as well as being skeptical of foreign hardware like unknown hard drives and floppy

discs that could give attackers access to critical software or systems. Maintaining data integrity using digital signatures, Wesley Chai states in his writing under paragraph two of the integrity section, “... provide effective nonrepudiation measures...” This maintains integrity of documents, messages, etc., sent by people. Restricting personnel access and editing rights for different share drives and documents to prevent tampering/alteration also helps keep data integrity. For organizations, data availability is maintained by keeping up with software updates, ensuring their hardware is properly stored and safeguarded, and conduct any repairs or necessary upgrades to said hardware. These are just a few examples needed to maintain availability. There should also be a quick recovery action plan in the event of data loss, a full back-up plan to recover data, preventing the organization from failing and allowing it to bounce back as fast as possible.

Authorization Vs. Authentication

Authorization is the act of giving someone access to restricted information. An organization called Fortinet defines authorization as, “... the process of giving a user permission to access a physical location or information-based resource (e.g., a document, database, application, or website).” Authentication is the process of identifying the authorized user trying to access restricted information, is who they say they are. Different methods are used, one example of authentication is biometric, where the authorized person uses a thumbprint to verify their identity. Another authentication method is two-factor authentication (2FA). In the writing “2 Factor Authentication vs 2 Step Verification: What’s The Difference?” Savvy Security states, “Two factor authentication... involves using two separate identifying “factors” to authenticate the user. Factors are things that people know, possess, or are attributes that are inherent to them as

individuals...” Some examples of these factors are a username and password (something you know), and your thumbprint (something you are).

Conclusion

The CIA Triad is a model comprised of the three foundational elements of cybersecurity. Covering each point on the triad, confidentiality, integrity, and availability will not only help an organization create its information security policies, but also ensure effective cybersecurity is being practiced. They are most crucial and without them, an organization would not be able to grow let alone function.

Wesley Chai:

[What is the CIA Triad Definition, Explanation, Examples - TechTarget.pdf - Google Drive](#)

Savvy Security:

[2 Factor Authentication vs 2 Step Verification: What's The Difference? \(cheapsslsecurity.com\)](#)

Fortinet:

[Authentication vs. Authorization: Key Differences | Fortinet](#)