The CIA Triad Explained

By: Paul Cumiskey

Bluff

The CIA Triad is a concept of information security that represents the three fundamental pillars of information security Confidentiality, Integrity, and Availability. The CIA triad encapsulates the tug-of-war between keeping data safe and accessible. The CIA triad is used as a framework to keep data safe, but not at the cost of loss of all availability. The CIA triad is used to help guide the development of security policies for organizations and has been a great benefit to cybersecurity as a whole while doing so.

Confidentiality

Confidentiality ensures that sensitive information is only accessible to authorized users. It protects data from unauthorized access and bad actors by implementing security measures. Maintaining confidentiality is critical to protect sensitive data such as personal data, company secrets, and classified information.

- **Confidentiality techniques**
    - **Encryption**: Protecting information by using a mathematical model to scramble it. The receiver of the information needs to have a key to unscramble it

- **Access controls**: Security process that allows organizations to manage who is authorized to what.
- **Multifactor authentication**: A security method that requires multiple forms of verification.

Integrity

Integrity ensures that data remains constantly accurate and trustworthy throughout its entire lifecycle. Integrity aims to prevent unauthorized modifications, intentional or not. This allows organizations to trust their data. It also prevents a plethora of cyber attacks that involve editing files on a system.

- **Integrity techniques**
  - **Hashing:** Converts data to a string of characters called a hash value. If the original data is changed the hash will also change.
  - **Checksums:** A value that is used to verify the integrity of a file
  - **Digital Signatures:** An electronic stamp of authentication on messages and documents

Availability

Availability ensures that information and resources are accessible to authorized users when needed. This is one of the most important and dynamic aspects of cybersecurity as a whole. While it is not impossible to have a completely safe network the usability of that network would be terrible. Availability aims to minimize downtime and ensure the system remains operational.

- **Availability techniques**
    - **Redundancy:** Using more than one device or system to maintain a service
    - **Failover Systems:** An operational mode that switches to a standby server or network if the system fails
    - **Regular Backups:** protects from losses due to hardware failure, human error, and cyber attacks

Conclusion

In conclusion, the CIA Triad is a critical framework in cybersecurity. It helps find the perfect balance between security and accessibility. The focus on confidentiality, integrity, and availability allows for data to be protected from threats while remaining useful. Today there are numerous bad actors and ever-evolving cyber threats; however, adhering to the CIA Triad's principles will help mitigate these threats.