Nishant Baruah A053 70022100516 BTech CE Batch 2

What is the CIA triad (confidentiality, integrity and availability)?

The CIA triad refers to confidentiality, integrity and availability, describing a model designed to guide policies for information security (infosec) within an organization. The model is sometimes referred to as the AIC triad -- which stands for availability, integrity and confidentiality -- to avoid confusion with the Central Intelligence Agency.

In this context, confidentiality is a set of high-level rules that limits access to all types of data and information. Integrity is the assurance that the information is trustworthy and accurate.
And availability is a form of risk management to guarantee reliable access to that information by authorized people.

What are the 3 components of the CIA triad?

1. **Confidentiality.** Roughly equivalent to privacy, confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It's common for data to be classified according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent data security measures can then be implemented according to those categories.
2. **Integrity.** The consistency, accuracy and trustworthiness of data must be maintained over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure it can't be altered by unauthorized people -- for example, in data breaches.
3. **Availability**. Information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

Nishant Baruah A053 70022100516 BTech CE Batch 2

Why is the CIA triad important?

Each letter in the CIA triad represents a foundational principle in cybersecurity. The importance of the security model speaks for itself: Confidentiality, integrity and availability are considered the three most important concepts in infosec.

Considering these three principles together within the triad framework guides the development of security policies for organizations. When evaluating needs and use cases for potential new products and technologies, the triad helps organizations ask focused questions about how value is being provided in those three key areas.

Thinking of the three concepts as an interconnected system, rather than as independent concepts, can help organizations understand the relationships between the three.

What are examples of the CIA triad?

Here are examples of the various management practices and technologies that constitute the CIA triad. While many CIA triad cybersecurity strategies implement these technologies and practices, this list is by no means exhaustive

Confidentiality

Sometimes safeguarding data confidentiality involves special training for those handling sensitive documents. Training can familiarize authorized people with risk factors and help them with risk assessments and to guard against those risks. Further aspects of training include strong passwords and password-related best practices, as well as information about social engineering methods bad actors use to get users to make mistakes and break data-handling rules.

A good example of a method for protecting sensitive data and ensuring confidentiality is requiring an account number or routing number when banking online. Data encryption is another common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure required for social media platforms, for example. Two-factor authentication (2FA) is also becoming commonplace in the healthcare and financial services industries.

Other options include real-time biometric verification, security tokens, key fobs and soft tokens. In addition, users can minimize the places where information appears and the number of times it's transmitted to complete a transaction. Extra measures might be taken in the case of extremely sensitive documents, such as storing only on air-gapped computers, on disconnected storage devices or in hard-copy form only.

Integrity

Measures related to data integrity include file permissions and user access controls. Version control is used to fix instances where an authorized user makes an erroneous change or accidental deletion. Organizations usually have some means to detect changes in data that occur as a result of non-human-caused events, such as an electromagnetic pulse or server crash.

Data might include checksums, even cryptographic checksums, for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state. Furthermore, digital signatures can be used to provide effective nonrepudiation measures, meaning evidence of logins, messages sent, and electronic document viewing and sending cannot be denied.

Availability

Rigorously maintaining hardware, performing hardware repairs immediately and maintaining a properly functioning operating system environment free of software conflicts are the best ways to ensure availability. It's also important to keep current with all system upgrades. Providing adequate communication bandwidth and preventing bottlenecks are also important tactics. Redundancy, failover, redundant array of independent disks (RAID) and even high availability clusters can mitigate serious consequences when hardware issues do occur.

Fast, adaptive disaster recovery (DR) plans are essential for the worst-case scenarios and require a comprehensive approach. Safeguards against data loss or interruptions in connections must include unpredictable events, such as power outages, natural disasters and fire. To prevent data loss from such occurrences, backup copies can be stored in a geographically isolated location or fireproof, waterproof safe. Extra security equipment and software, such as firewalls and proxy servers, can guard against downtime. They also help prevent security incidents that result in unreachable data blocked by malicious denial-of-service attacks, ransomware and other malware or cyber attacks.