techtarget.com

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

Wesley Chai

10–12 minutes

-
-

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency. Although elements of the triad are three of the most foundational and crucial cybersecurity needs, experts believe the CIA triad

needs an upgrade to stay effective.

In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

The following is a breakdown of the three key concepts that form the CIA triad:

- **Confidentiality** is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be implemented according to those categories.
- **Integrity** involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a

breach of confidentiality).

- **Availability** means 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.

The three CIA triad principles

Why is the CIA triad important?

With each letter representing a foundational principle in cybersecurity, the importance of the CIA triad security model speaks for itself. Confidentiality, integrity and availability together are considered the three most important concepts within information security.

Considering these three principles together within the framework of the "triad" can help guide 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 CIA triad's three concepts together 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 comprise 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 privy to sensitive

documents. Training can help familiarize authorized people with risk factors and how to guard against them. Further aspects of training may include strong passwords and password-related best practices and information about social engineering methods to prevent users from bending data-handling rules with good intentions and potentially disastrous results.

A good example of methods used to ensure 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; two-factor authentication (2FA) is becoming the norm. Other options include Biometric verification and security tokens, key fobs or soft tokens. In addition, users can take precautions to minimize the number of places where information appears and the number of times it is actually transmitted to complete a required transaction. Extra measures might be taken in the case of extremely sensitive

documents, such as storing only on air-gapped computers, disconnected storage devices or, for highly sensitive information, in hard-copy form only.

Integrity

These measures include file permissions and user access controls. Version control may be used to prevent erroneous changes or accidental deletion by authorized users from becoming a problem. In addition, organizations must put in some means to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) 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, electronic document viewing and sending cannot be denied.

Availability

This is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a properly functioning operating system (OS) environment that is free of software conflicts. It's also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important tactics. Redundancy, failover, RAID -- even high-availability clusters -- can mitigate serious consequences when hardware issues do occur.

Fast and adaptive disaster recovery is essential for the worst-case scenarios; that capacity relies on the existence of a comprehensive DR plan. Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a backup copy may be stored in a geographically isolated location, perhaps even in a fireproof, waterproof safe. Extra

security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data blocked by malicious denial-of-service (DoS) attacks and network intrusions.

What are challenges for the CIA triad?

Big data poses challenges to the CIA paradigm because of the sheer volume of information that organizations need safeguarded, the multiplicity of sources that data comes from and the variety of formats in which it exists. Duplicate data sets and disaster recovery plans can multiply the already-high costs. Furthermore, because the main concern of big data is collecting and making some kind of useful interpretation of all this information, responsible data oversight is often lacking. Whistleblower Edward Snowden brought that problem to the public forum when he reported on the National Security Agency's collection of massive volumes of American citizens' personal data.

Internet of things privacy protects the information of

individuals from exposure in an IoT environment. Almost any physical or logical entity or object can be given a unique identifier and the ability to communicate autonomously over the internet or a similar network. The data transmitted by a given endpoint might not cause any privacy issues on its own. However, when even fragmented data from multiple endpoints is gathered, collated and analyzed, it can yield sensitive information.

Internet of things security is also challenging because IoT consists of so many internet-enabled devices other than computers, which often go unpatched and are often configured with default or weak passwords. Unless adequately protected, IoT could be used as a separate attack vector or part of a thingbot.

As more and more products are developed with the capacity to be networked, it's important to routinely consider security in product development.

What are best practices for implementing the CIA triad?

In implementing the CIA triad, an organization should follow a general set of best practices. Some best practices, divided by each of the three subjects, include:

Confidentiality

- Data should be handled based on the organization's required privacy.
- Data should be encrypted using 2FA.
- Keep access control lists and other file permissions up to date.

Integrity

- Ensure employees are knowledgeable about compliance and regulatory requirements to minimize human error.
- Use backup and recovery software.
- To ensure integrity, use version control, access control, security control, data logs and checksums.

Availability

- Use preventive measures such as redundancy, failover and RAID. Ensure systems and

applications stay updated.

- Use network or server monitoring systems.
- Ensure a data recovery and business continuity (BC) plan is in place in case of data loss.

What is the history of the CIA triad?

The concept of the CIA triad formed over time and does not have a single creator. Confidentiality may have first been proposed as early as 1976 in a study by the U.S. Air Force. Likewise, the concept of integrity was explored in a 1987 paper titled "A Comparison of Commercial and Military Computer Security Policies" written by David Clark and David Wilson. The paper recognized that commercial computing had a need for accounting records and data correctness. Even though it is not as easy to find an initial source, the concept of availability became more widespread one year later in 1988.

By 1998, people saw the three concepts together as the CIA triad.

This was last updated in February 2023

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

- How to secure data at rest, in use and in motion
- Symmetric vs. asymmetric encryption: Decipher the differences
- How to develop a cybersecurity strategy: A step by step guide