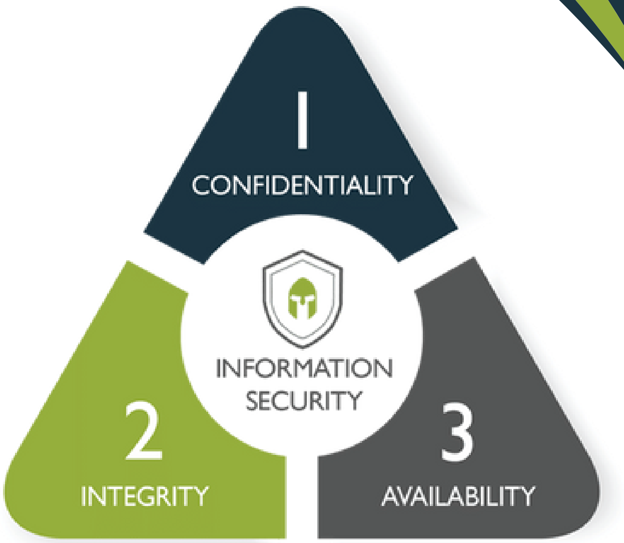
CIA Triad



Created By : Farhath Nathvi
LinkedIn

www.linkedin.com/in/farhathnathvi

CIA Triad

The CIA triad is a framework that combines three key information security principles: confidentiality, integrity, and availability.

The CIA triad provides a simple and complete checklist for evaluating an organization's security. An effective IT security system consists of three parts: confidentiality, integrity, and availability, hence the name "CIA triad."

More than an information security framework, the CIA triad helps organizations upgrade and maintain maximum security while enabling staff to perform everyday tasks like data collection, customer service, and general management.

This guide will take you through each of the three components of CIA triad and examples to help bring them to life.

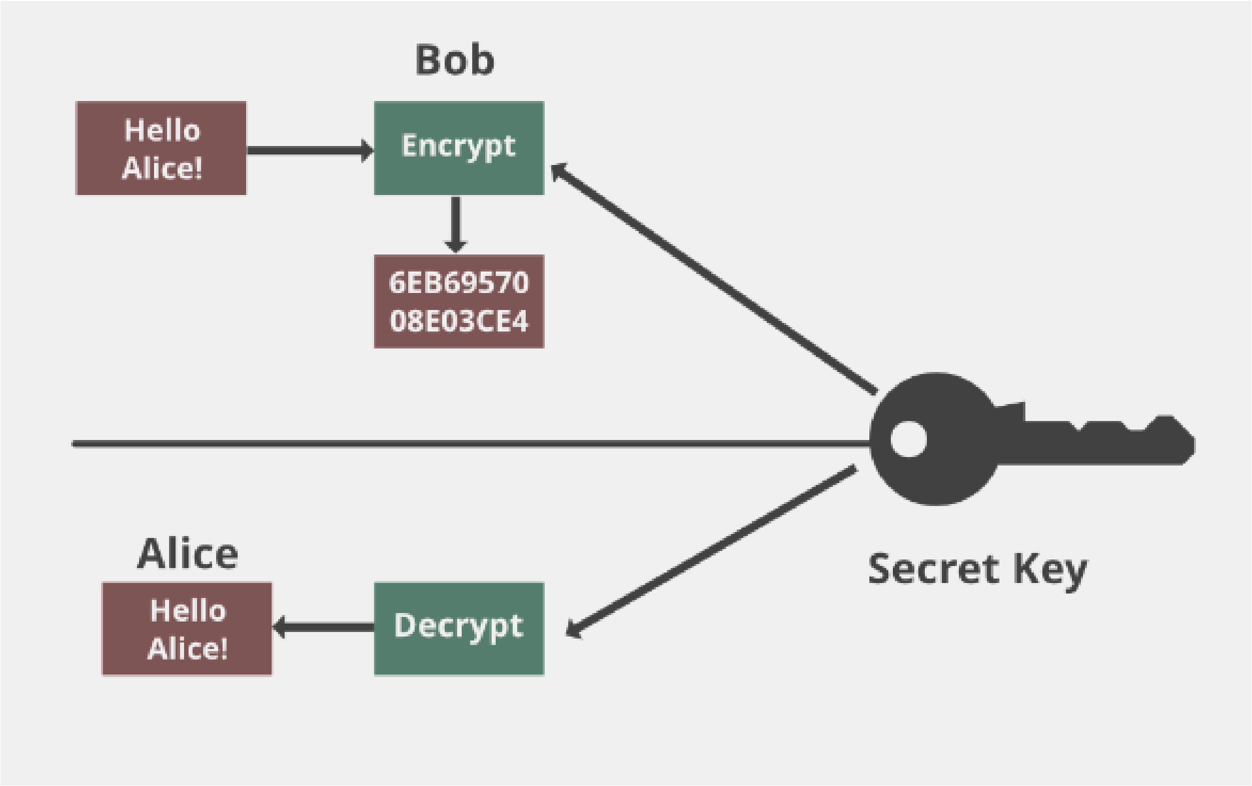
What is the CIA triad?

The CIA triad provides a high-level framework for cybersecurity professionals to consider when auditing, implementing, and improving systems, tools, and programs for organizations. It is a powerful way to identify weak points and form solutions to strengthen policies and programs.

Let's take a closer look at the three elements of the triad.

1. Confidentiality

Confidentiality means that only authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet and gain access to your information. A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to your data, he/she will not be able to decrypt it. Encryption standards include AES(Advanced Encryption Standard) and DES (Data Encryption Standard). Another way to protect your data is through a VPN tunnel. VPN stands for Virtual Private Network and helps the data to move securely over the network.

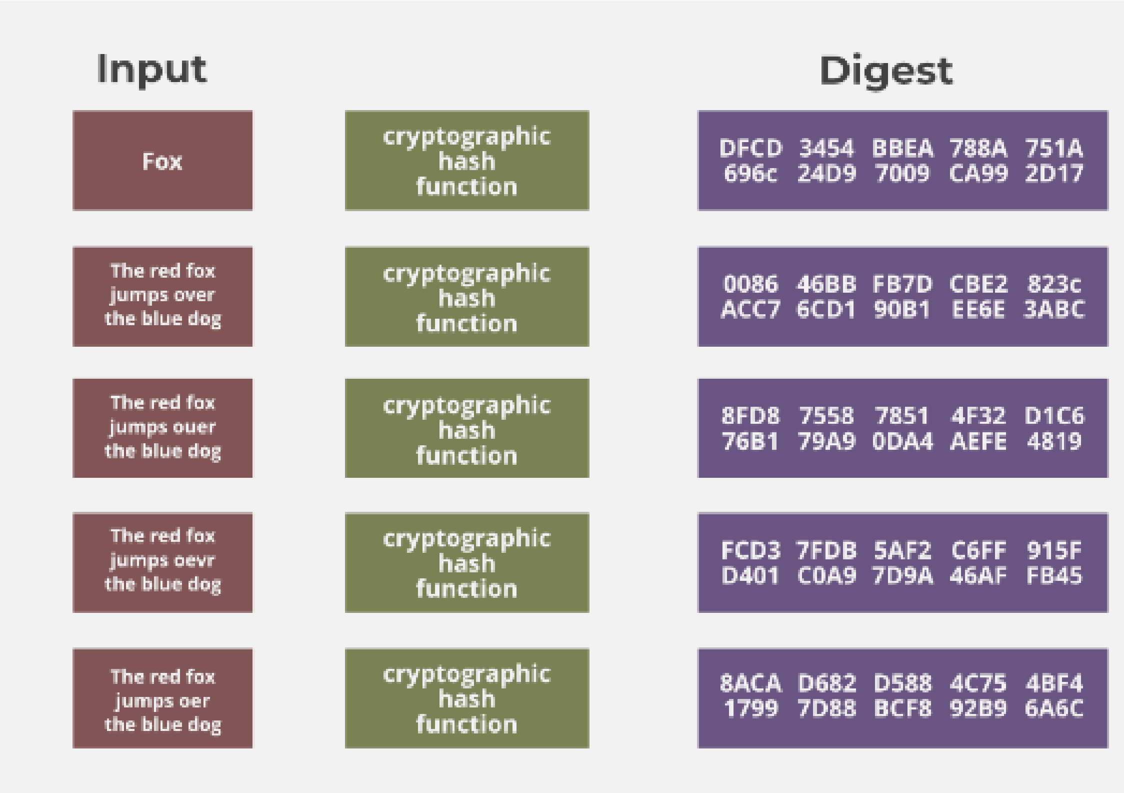


2. Integrity

The next thing to talk about is integrity. Well, the idea here is to make sure that data has not been modified. Corruption of data is a failure to maintain data integrity. To check if our data has been modified or not, we make use of a hash function.

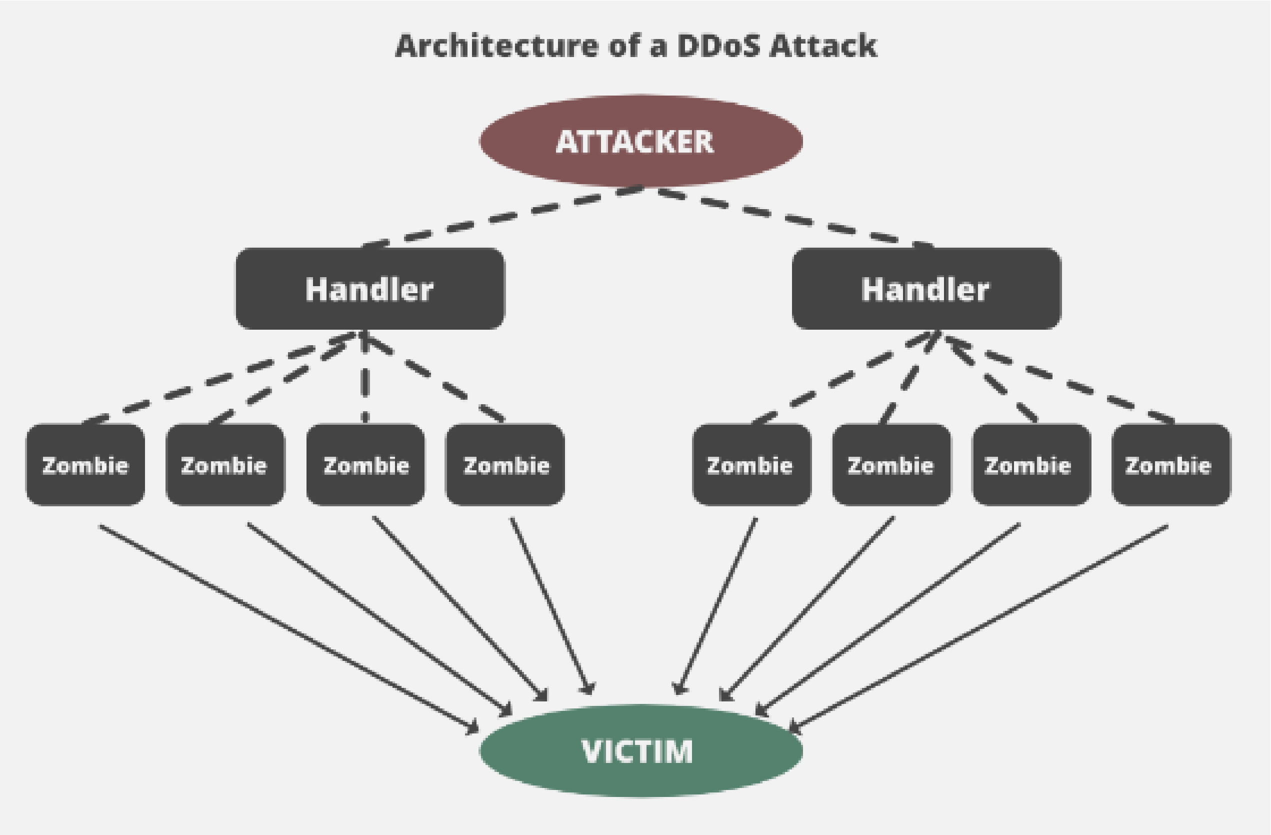
We have two common types: SHA (Secure Hash Algorithm) and MD5(Message Direct 5). Now MD5 is a 128-bit hash and SHA is a 160-bit hash if we're using SHA-1. There are also other SHA methods that we could use like SHA-0, SHA-2, and SHA-3.

Let's assume Host 'A' wants to send data to Host 'B' to maintain integrity. A hash function will run over the data and produce an arbitrary hash value H1 which is then attached to the data. When Host 'B' receives the packet, it runs the same hash function over the data which gives a hash value of H2. Now, if H1 = H2, this means that the data's integrity has been maintained and the contents were not modified.


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696c 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823c ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

3. Availability

This means that the network should be readily available to its users. This applies to systems and to data. To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over, and prevent bottlenecks in a network. Attacks such as DoS or DDoS may render a network unavailable as the resources of the network get exhausted. The impact may be significant to the companies and users who rely on the network as a business tool. Thus, proper measures should be taken to prevent such attacks.



Why is the CIA triad important?

Because information security covers so many areas, it’s crucial to have one methodology to analyze situations, plan changes, and improve implementations. The CIA triad gives leaders a way to think about security challenges without being security experts. It helps data professionals assess what went wrong during a malfunction or cybersecurity attack and how it can be fixed.

What are examples of the CIA triad?

Information security professionals often need to consider confidentiality, integrity, and availability in their organizations. These examples help you think through the three components of the CIA triad to make your system more robust.

Examples of confidentiality

An organization’s data should only be available to those who need it. Access to data such as human resources files, medical records, and school transcripts should be limited.

To prevent security breaches, confidentiality policies must be followed so access is limited only to authorized users. Data can be classified, labelled, or encrypted to allow restrictions. The IT team can implement multi-factor authentication systems. Employees can receive onboarding training to recognize potential security mistakes and how to avoid them.

Effective information security considers who receives authorization and the appropriate level of confidentiality. For example, the finance team of an organization should be able to access bank accounts, but most other employees and executives should not have access to this information. Some security measures include locked cabinets to limit access to physical files and encrypted digital files to protect information from hackers.

Confidentiality can be compromised unintentionally. For example, IT support might accidentally send a password to multiple employees, instead of the one who needs it. Users might share their credentials with another employee, or forget to properly encrypt a sensitive email. A thief might steal an employee's hardware, such as a computer or mobile phone. Insufficient security controls or human error are also examples of breached confidentiality.

Examples of Integrity

An information system with integrity tracks and limits who can make changes to minimize the possible damage that hackers, malicious employees, or human errors can do.

Organizations need to determine who can change the data and how it can be changed. For example, schools typically protect grade databases so students can’t change them but teachers can. In this case, a student hacker might bypass the intrusion detection system or alter system logs to mask the attack after it occurs.

Information on an organization's website should be trustworthy. In another example, a company website that provides bios of senior executives must have integrity. If it is inaccurate or seems botched, visitors may be reluctant to trust the company or buy its products. If the company has a high profile, a competitor might try to damage its reputation by hacking the website and altering descriptions.

To protect data integrity, encryption, digital signatures, and hashing can be used. Websites can use certificate authorities that verify its authenticity so customers feel comfortable browsing and purchasing products.

Examples of availability

All organizations have designated employees with access to specific data and permission to make changes. Therefore, security framework must include availability.

Information security professionals must balance availability with confidentiality and integrity. For example, all employees of an organization might have access to the company email system, but detailed financial records may only be made available to top-level leadership. Those leaders should be able to access that data when they need to, and it shouldn't take too much time or effort to access it.

Backup systems should be in place to allow for availability. For example, disaster recovery systems need to be implemented so employees can regain access to data systems if there is a power outage. Or, if a natural disaster such as a hurricane or snowstorm prevents employees from physically getting to the office, their data be available to them through cloud system storage.

Availability can be compromised through sabotage. For example, sabotage can occur through denial-of-service attacks or ransomware. To maintain data availability, organizations can use "redundant" networks and servers that are programmed to become available when the default system breaks or gets tampered with. Updating and upgrading systems on a regular basis prevents infiltrations and malfunctions which enhance data availability.

Benefits of the CIA triad

The CIA triad provides multiple benefits to businesses, especially to ones that deal with sensitive data. The benefits of triad implementation include the following:

- **Data security and privacy.** The most obvious benefit is ensuring preparedness in the face of today's sophisticated cyber attacks and other unauthorized attempts to access, steal or manipulate valuable data.

- **Compliance.** Ensuring the confidentiality, integrity and availability of sensitive information means regulations and legal frameworks that exist to safeguard this information are followed.

- **Proactive risk prevention.** When applied correctly, the triad creates an environment where security risks are proactively prevented. Existing vulnerabilities are identified and mitigated to prevent future threats.

- **Comprehensiveness.** The three components mean that security teams aren't just concerned with thwarting attackers, but they're also ensuring the veracity and availability of their data. For example, when a large volume of data is needed for analysis, following the CIA triad means the data is available and accessible when needed.

Risks of Ignoring the CIA Triad

Ignoring the CIA Triad—Confidentiality, Integrity, and Availability—poses significant risks to organizations and individuals alike. The CIA Triad is a foundational model in cybersecurity, ensuring that data is protected from unauthorized access, remains accurate and trustworthy, and is available when needed. Failing to address any of these aspects can lead to the following risks:

1. Compromised Confidentiality:

- **Unauthorized Access:** Sensitive information, such as personal data, financial records, or intellectual property, may be accessed by unauthorized individuals. This can lead to data breaches, identity theft, or loss of competitive advantage.

- **Privacy Violations:** Failure to protect confidentiality can result in non-compliance with data protection regulations (e.g., GDPR), leading to legal consequences, fines, and reputational damage.

2. Loss of Integrity:

- **Data Tampering**: If the integrity of data is not ensured, information can be altered, leading to inaccurate or misleading data. This can have severe consequences in sectors like healthcare, finance, or legal, where accurate data is crucial.

- **Fraud and Manipulation**: Cyber attackers can exploit weak integrity controls to manipulate data for fraudulent activities, such as financial fraud, misinformation campaigns, or sabotaging systems.

3. Disrupted Availability:

- **Downtime and Unavailability:** Ignoring the availability aspect can result in systems being unavailable when needed, disrupting business operations, leading to financial losses, and affecting customer trust.

- **Denial of Service (DoS) Attacks:** Without proper availability safeguards, systems are vulnerable to DoS or DDoS attacks, where attackers overwhelm systems with traffic, making them inaccessible to legitimate users.

4. Reputational Damage:

- **Loss of Trust:** Clients, partners, and customers lose trust in an organization that fails to protect its data. This can lead to a loss of business, customer churn, and difficulties in attracting new customers.

- **Negative Publicity:** Data breaches, system failures, or privacy violations often lead to negative media coverage, which can tarnish the organization's public image.

5. Legal and Regulatory Consequences:

- **Compliance Violations:** Many industries have strict regulations regarding data protection. Ignoring the CIA Triad can lead to non-compliance, resulting in heavy fines, legal actions, and even business shutdowns.

- **Litigation Risk:** Organizations may face lawsuits from affected parties, including customers, partners, or shareholders, if they fail to protect data according to the CIA Triad principles.

6. Financial Loss:

- **Cost of Data Breaches:** The financial impact of a data breach can be enormous, including costs associated with incident response, remediation, legal fees, and regulatory fines.
- **Operational Costs:** Downtime and data loss can disrupt business operations, leading to a significant reduction in revenue and increased recovery costs.

7. National Security Threats:

- Critical Infrastructure Attacks: Ignoring the CIA Triad in critical infrastructure sectors (e.g., energy, healthcare, transportation) can lead to devastating consequences, including national security risks and endangering public safety.

In summary, neglecting the CIA Triad can lead to a cascade of negative outcomes, from data breaches and financial losses to legal penalties and reputational harm. Organizations must prioritize all three aspects to ensure comprehensive cybersecurity and safeguard their assets and stakeholders.

Best practices for implementing the CIA triad

In implementing the CIA triad, an organization should follow a general set of best practices. These can be divided into the three subjects and include the following:

1. **Confidentiality**
    - Follow an organization's data-handling security policies.
    - Use encryption and 2FA.
    - Keep access control lists and other file permissions up to date.

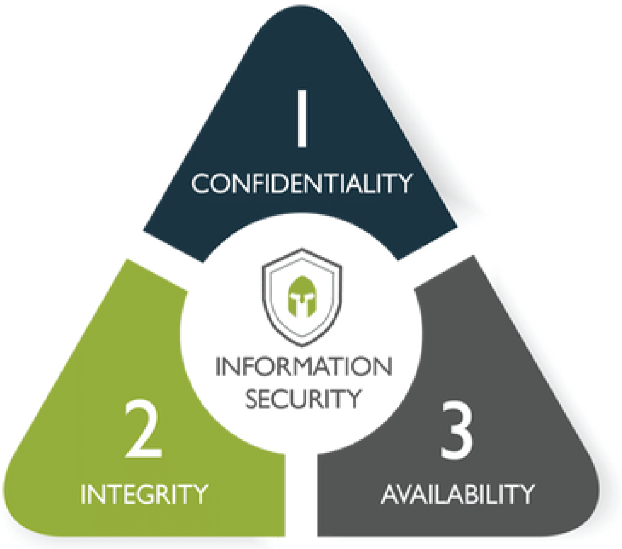
1. **Integrity**
    - Ensure employees are knowledgeable about compliance and regulatory requirements to minimize human error.
    - Use backup and recovery software and services.
    - Use version control, access control, security control, data logs and checksums.

1. **Availability**
    - Use preventive measures, such as redundancy, failover and RAID.
    - Ensure systems and applications stay updated.
    - Use network or server monitoring systems.
    - Have a data recovery and business continuity plan in place in case of data loss.

The history of the CIA triad

The concept of the CIA Triad is shaped over time and does not have a single creator. "Confidentiality" appeared in 1976 in a study in the U.S. Air Force. The concept of "Integrity" is found in a 1987 dissertation titled "A Comparison of Commercial and Military Computer Security Policies" written by David Clark and David Wilson. The dissertation stated that in commercial data processing, methods are needed to ensure the accuracy of data. As for "Availability", there is no clear initial source, but the concept became well known in 1988, which was also the year when the three components were brought together and formed the concept of the CIA Triad.

CIA Triad



Thank you