csoonline.com

The CIA triad: Definition, components and examples

by Josh Fruhlinger Contributing writer

11–14 minutes

Feature

Feb 10, 202010 mins

Data and Information SecuritySecurity

Information security relies on keeping data secure, integral, and available—but tradeoffs are necessary in real-world scenarios.

What is the CIA triad? The CIA triad components, defined

The *CIA triad* is a widely used information security model that can guide an organization's efforts and policies aimed at keeping its data secure. The

model has nothing to do with the U.S. Central Intelligence Agency; rather, the initials stand for the three principles on which infosec rests:

- **Confidentiality:** Only authorized users and processes should be able to access or modify data
- **Integrity:** Data should be maintained in a correct state and nobody should be able to improperly modify it, either accidentally or maliciously
- **Availability:** Authorized users should be able to access data whenever they need to do so

These three principles are obviously top of mind for any infosec professional. But considering them as a triad forces security pros to do the tough work of thinking about how they overlap and can sometimes be in opposition to one another, which can help in establishing priorities in the implementation of security policies. We'll discuss each of these principles in more detail in a moment, but first let's talk about the origins and importance of the triad.

Who created the CIA triad, and when?

Unlike many foundational concepts in infosec, the CIA triad doesn't seem to have a single creator or proponent; rather, it emerged over time as an article of wisdom among information security pros. Ben Miller, a VP at cybersecurity firm Dragos, traces back early mentions of the three components of the triad in a blog post; he thinks the concept of confidentiality in computer science was formalized in a 1976 U.S. Air Force study, and the idea of integrity was laid out in a 1987 paper that recognized that commercial computing in particular had specific needs around accounting records that required a focus on data correctness. Availability is a harder one to pin down, but discussion around the idea rose in prominence in 1988 when the Morris worm, one of the first widespread pieces of malware, knocked a significant portion of the embryonic internet offline.

It's also not entirely clear when the three concepts began to be treated as a three-legged stool. But it seems to have been well established as a foundational concept by 1998, when Donn Parker,

in his book Fighting Computer Crime, proposed extending it to a six-element framework called the Parkerian Hexad. (We'll return to the Hexad later in this article.)

Thus, CIA triad has served as a way for information security professionals to think about what their job entails for more than two decades. The fact that the concept is part of cybersecurity lore and doesn't "belong" to anyone has encouraged many people to elaborate on the concept and implement their own interpretations.

Why is the CIA triad important?

Anyone familiar with even the basics of cybersecurity would understand why these three concepts are important. But why is it so helpful to think of them as a triad of linked ideas, rather than separately?

It's instructive to think about the CIA triad as a way to *make sense* of the bewildering array of security software, services, and techniques that are in the marketplace. Rather than just throwing money and

consultants at the vague “problem” of “cybersecurity,” we can ask focused questions as we plan and spend money: Does this tool make our information more secure? Does this service help ensure the integrity of our data? Will beefing up our infrastructure make our data more readily available to those who need it?

In addition, arranging these three concepts in a triad makes it clear that they exist, in many cases, in tension with one another. We’ll dig deeper into some examples in a moment, but some contrasts are obvious: Requiring elaborate authentication for data access may help ensure its confidentiality, but it can also mean that some people who have the right to see that data may find it difficult to do so, thus reducing availability. Keeping the CIA triad in mind as you establish information security policies forces a team to make productive decisions about which of the three elements is most important for specific sets of data and for the organization as a whole.

CIA triad examples

To understand how the CIA triad works in practice, consider the example of a bank ATM, which can offer users access to bank balances and other information. An ATM has tools that cover all three principles of the triad:

- It provides **confidentiality** by requiring two-factor authentication (both a physical card and a PIN code) before allowing access to data
- The ATM and bank software enforce data **integrity** by ensuring that any transfers or withdrawals made via the machine are reflected in the accounting for the user's bank account
- The machine provides **availability** because it's in a public place and is accessible even when the bank branch is closed

But there's more to the three principles than just what's on the surface. Here are some examples of how they operate in everyday IT environments.

CIA triad confidentiality examples

Much of what laypeople think of as "cybersecurity"

— essentially, anything that restricts access to data — falls under the rubric of confidentiality. This includes infosec's two big As:

- *Authentication*, which encompasses processes that allows systems to determine if a user is who they say they are. These include passwords and the panoply of techniques available for establishing identity: biometrics, security tokens, cryptographic keys, and the like.
- *Authorization*, which determines who has the right to access which data: Just because a system knows who you are, it doesn't necessarily open all its data for your perusal! One of the most important ways to enforce confidentiality is establishing need-to-know mechanisms for data access; that way, users whose accounts have been hacked or who have gone rogue can't compromise sensitive data. Most operating systems enforce confidentiality in this sense by having many files only accessible by their creators or an admin, for instance.

  Public-key cryptography is a widespread infrastructure that enforces both As: by

authenticating that you are who you say you are via cryptographic keys, you establish your right to participate in the encrypted conversation.

Confidentiality can also be enforced by non-technical means. For instance, keeping hardcopy data behind lock and key can keep it confidential; so can air-gapping computers and fighting against social engineering attempts.

A loss of confidentiality is defined as data being seen by someone who shouldn't have seen it. Big data breaches like the Marriott hack are prime, high-profile examples of loss of confidentiality.

CIA triad integrity examples

The techniques for maintaining data integrity can span what many would consider disparate disciplines. For instance, many of the methods for protecting confidentiality also enforce data integrity: you can't maliciously alter data that you can't access, after all. We also mentioned the data access rules enforced by most operating systems: in some cases, files can be read by certain users

but not edited, which can help maintain data integrity along with availability.

But there are other ways data integrity can be lost that go beyond malicious attackers attempting to delete or alter it. For instance, corruption seeps into data in ordinary RAM as a result of interactions with cosmic rays much more regularly than you'd think. That's at the exotic end of the spectrum, but any techniques designed to protect the physical integrity of storage media can also protect the virtual integrity of data.

Many of the ways that you would defend against breaches of integrity are meant to help you detect when data has changed, like data checksums, or restore it to a known good state, like conducting frequent and meticulous backups. Breaches of integrity are somewhat less common or obvious than violations of the other two principles, but could include, for instance, altering business data to affect decision-making, or hacking into a financial system to briefly inflate the value of a stock or bank account and then siphoning off the excess. A

simpler — and more common — example of an attack on data integrity would be a defacement attack, in which hackers alter a website's HTML to vandalize it for fun or ideological reasons.

CIA triad availability examples

Maintaining availability often falls on the shoulders of departments not strongly associated with cybersecurity. The best way to ensure that your data is available is to keep all your systems up and running, and make sure that they're able to handle expected network loads. This entails keeping hardware up-to-date, monitoring bandwidth usage, and providing failover and disaster recovery capacity if systems go down.

Other techniques around this principle involve figuring out how to balance the availability against the other two concerns in the triad. Returning to the file permissions built into every operating system, the idea of files that can be read but not edited by certain users represent a way to balance competing needs: that data be available to many

users, despite our need to protect its integrity.

The classic example of a loss of availability to a malicious actor is a denial-of-service attack. In some ways, this is the most brute force act of cyberaggression out there: you're not altering your victim's data or sneaking a peek at information you shouldn't have; you're just overwhelming them with traffic so they can't keep their website up. But DoS attacks are very damaging, and that illustrates why availability belongs in the triad.

CIA triad implementation

The CIA triad should guide you as your organization writes and implements its overall security policies and frameworks. Remember, implementing the triad isn't a matter of buying certain tools; the triad is a way of thinking, planning, and, perhaps most importantly, setting priorities. Industry standard cybersecurity frameworks like the ones from NIST (which focuses a lot on integrity) are informed by the ideas behind the CIA triad, though each has its own

particular emphasis.

Beyond the triad: The Parkerian Hexad, and more

The CIA triad is important, but it isn't holy writ, and there are plenty of infosec experts who will tell you it doesn't cover everything. As we mentioned, in 1998 Donn Parker proposed a six-sided model that was later dubbed the Parkerian Hexad, which is built on the following principles:

- Confidentiality
- Possession or control
- Integrity
- Authenticity
- Availability
- Utility

It's somewhat open to question whether the extra three points really press into new territory — utility and possession could be lumped under availability, for instance. But it's worth noting as an alternative

model.

A final important principle of information security that doesn't fit neatly into the CIA triad is *non-repudiation,* which essentially means that someone cannot falsely deny that they created, altered, observed, or transmitted data. This is crucial in legal contexts when, for instance, someone might need to prove that a signature is accurate, or that a message was sent by the person whose name is on it. The CIA triad isn't a be-all and end-all, but it's a valuable tool for planning your infosec strategy.