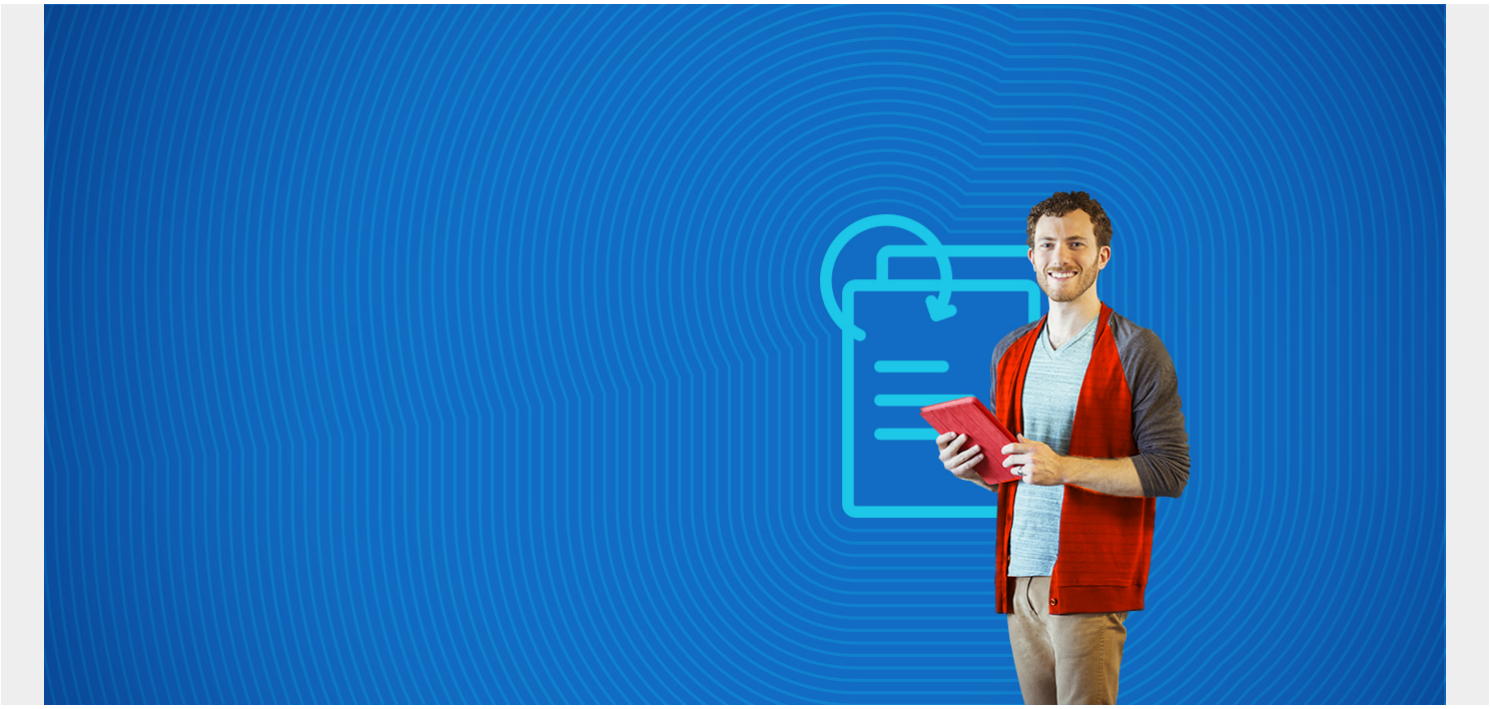
WHAT IS THE CIA SECURITY TRIAD? CONFIDENTIALITY, INTEGRITY, AVAILABILITY EXPLAINED

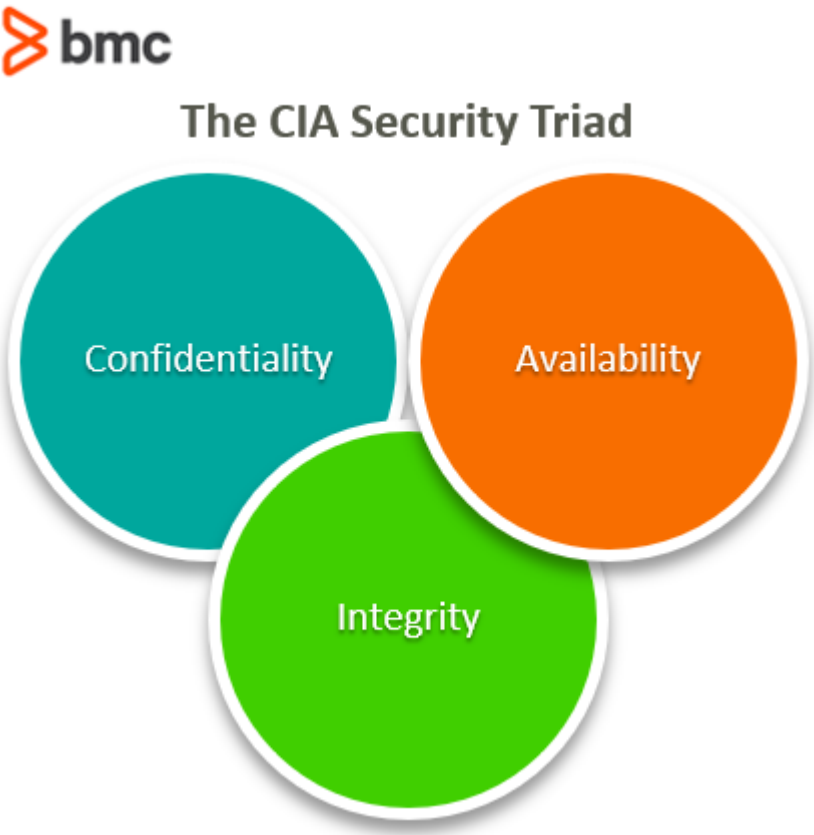


It's easy to protect some data that is valuable to you only. You could store your pictures or ideas or notes on an encrypted thumb drive, locked away in a spot where only you have the key.

But companies and organizations have to deal with this on a vast scale. After all, it's the company data—products, customer and employee details, ideas, research, experiments—that make your company useful and valuable. (The "assets" we normally think of, like hardware and software, are simply the tools that allow you to work with and save your company data.)

So, how does an organization go about protecting this data? Certainly, there's security strategies and technology solutions that can help, but one concept underscores them all: The CIA Security Triad.

This concept combines three components—confidentiality, integrity, and availability—to help guide security measures, controls, and overall strategy. Let's take a look.



(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

Defining CIA in cyber security

The CIA triad represents the functions of your information systems. Your information system encompasses both your computer systems and your data. Ben Dynkin, Co-Founder & CEO of Atlas Cybersecurity, explains that these are the functions that can be attacked—which means these are the functions you must defend.

The CIA security triad is comprised of three functions:

- **Confidentiality.** A system's ability to ensure that only the correct, authorized user/system/resource can view, access, change, or otherwise use data.
- **Integrity.** A system's ability to ensure that the system and information is accurate and correct.
- **Availability.** A system's ability to ensure that systems, information, and services are available the vast majority of time.

Let's look at each in more details.

Confidentiality in CIA Triad

In a non-security sense, confidentiality is your ability to keep something secret. In the real world, we might hang up blinds or put curtains on our windows. We might ask a friend to keep a secret. Confidentiality also comes into play with technology. It can play out differently on a personal-use level, where we use VPNs or encryption for our own privacy-seeking sake. We might turn off in-home devices that are always listening.

But in enterprise security, confidentiality is breached when an unauthorized person can view, take, and/or change your files. Confidentiality is significant because your company wants to protect its

competitive edge—the intangible assets that make your company stand out from your competition.

Integrity in CIA Triad

In computer systems, integrity means that the results of that system are precise and factual. In the data world, it's known as data trustworthiness—can you trust the results of your data, of your computer systems?

When securing any information system, integrity is one function that you're trying to protect. You don't want bad actors or human error to, on purpose or accidentally, ruin the integrity of your computer systems and their results.

Availability in CIA Triad

Availability is a term widely used in IT—the availability of resources to support your services. In security, availability means that the right people have access to your information systems. If a user with privileged access has no access to her dedicated computer, then there is no availability.

Availability is a large issue in security because it can be attacked. An attack on your availability could limit user access to some or all of your services, leaving you scrambling to clean up the mess and limit the downtime.

The CIA triad in enterprise security

OK, so we have the concepts down, but what do we do with the triad?

At its core, the CIA triad is a security model that you can—should—follow in order to protect information stored in on-premises computer systems or in the cloud. It helps you:

- Keep information secret (Confidentiality)
- Maintain the expected, accurate state of that information (Integrity)
- Ensure your information and services are up and running (Availability)

It's a balance: no security team can 100% ensure that confidentiality, integrity, and availability can never be breached, no matter the cause.

Instead, security professionals use the CIA triad to understand and assess your organizational risks. Dynkin suggests breaking down every potential threat, attack, and vulnerability into any one function of the triad. For example:

- A data breach attacks the confidentiality of your data.
- A ransomware incident attacks the availability of your information systems.

Understanding what is being attacked is how you can build protection against that attack. Take the case of ransomware—all security professionals want to stop ransomware. Where we tend to view ransomware broadly, as some "esoteric malware attack", Dynkin says we should view it as an attack designed specifically to limit your availability.

When you think of this as an attempt to limit availability, he told me, you can take additional mitigation steps than you might have if you were only trying to "stop ransomware".

The triad can help you drill down into specific controls. It also applies at a strategy and policy level. Dynkin continues: When you understand the CIA triad, you can expand your view of security "beyond the specific minutiae (which is still critically important) and focus on an organizational approach to information security."

Prioritize each thing you need to protect based on how severe the consequences would be if confidentiality, integrity, or availability were breached. For example, how might each event here breach one part or more of the CIA triad:

- **A service interruption:** An attacker could interrupt your access as a bargaining chip for something else.
- **Interception:** An attacker could block or hijack your emails to learn about company activity.
- **Modification or fabrication:** An attacker could modify or fake your information.

What if some incident can breach two functions at once? Consider, plan for, and take actions in order to improve each security feature as much as possible. For example, having backups—redundancy—improves overall availability. If some system's availability is attacked, you already have a backup ready to go.

CIA triad in action

You'll know that your security team is putting forth some security for the CIA triad when you see things like:

- Limits on administrator rights
- Inability to use your own, unknown devices
- The use of VPN to access certain sensitive company information

Anything that is an asset—tangible hardware and software, intangible knowledge and talent—should in some way be protected by your security team. And that is the work of the security team: to protect any asset that the company deems valuable. And it's clearly not an easy project.

Additional security properties

Security professionals already know that computer security doesn't stop with the CIA triad. ISO-7498-2 also includes additional properties for computer security:

- **Authentication:** The ability of your systems to confirm an identity.
- **Non-repudiation or accountability:** The ability of your systems to confirm the validity of something that occurs over the system. It is an assurance about data's origins and integrity.

Confidentiality, integrity, availability

These three components are the cornerstone for any security professional, the purpose of any security team. John Svazic, Founder of EliteSec, says that the CIA triad "acts as touchpoints for any type of security work being performed". That is, it's a way for SecOps professionals to answer:

How is the work we're doing actively improving one of these factors?

When your company builds out a security program, or adds a security control, you can use the CIA triad to justify the need for controls you're implementing. Always draw your security actions back to one or more of the CIA components.

That's why Svazic considers the CIA triad "a useful 'yardstick'" that helps you ensure the controls you are implementing are actually useful and necessary—not a placebo.

Related reading

- BMC Security & Compliance Blog
- Top 8 Ways Hackers Will Exfiltrate Data From Your Mainframe
- IT Asset Management: 10 Best Practices for Successful ITAM