confidentiality, integrity, availability (CIA)

What is it?

You may have heard information security specialists referring to the "CIA" -- but they're usually not talking about the Central Intelligence Agency or the Culinary Institute of America.

CIA is a widely used benchmark for evaluation of information systems security, focusing on the three core goals of confidentiality, integrity and availability of information.

Data confidentiality

Confidentiality refers to limiting information access and disclosure to authorized users -- "the right people" -- and preventing access by or disclosure to unauthorized ones -- "the wrong people."

Underpinning the goal of confidentiality are authentication methods like user-IDs and passwords, that uniquely identify a data system's users, and supporting control methods that limit each identified user's access to the data system's resources.

Also critical to confidentiality -- and data integrity and availability as well -- are protections against malicious software (malware), spyware, spam and phishing attacks.

Confidentiality is related to the broader concept of data privacy -- limiting access to individuals' personal information. In the US, a range of state and federal laws, with abbreviations like FERPA, FSMA, and HIPAA, set the legal terms of privacy.

Data integrity

Integrity refers to the trustworthiness of information resources.

It includes the concept of "data integrity" -- namely, that data have not been changed inappropriately, whether by accident or deliberately malign activity. It also includes "origin" or "source integrity" -- that is, that the data actually came from the person or entity you think it did, rather than an imposter.

Integrity can even include the notion that the person or entity in question entered the right information -- that is, that the information reflected the actual circumstances (in statistics, this is the concept of "validity") and that under the same circumstances

would generate identical data (what statisticians call "reliability").

On a more restrictive view, however, integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong.

Data availability

Availability refers, unsurprisingly, to the availability of information resources. An information system that is not available when you need it is at least as bad as none at all. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure.

Almost all modern organizations are highly dependent on functioning information systems. Many literally could not operate without them.

Availability, like other aspects of security, may be affected by purely technical issues (e.g., a malfunctioning part of a computer or communications device), natural phenomena (e.g., wind or water), or human causes (accidental or deliberate).

While the relative risks associated with these categories depend on the particular context, the general rule is that humans are the weakest link. (That's why each user's ability and willingness to use a data system securely are critical.)

Prevention vs. detection

Security efforts to assure confidentiality, integrity and availability can be divided into those oriented to prevention and those focused on detection. The latter aims to rapidly discover and correct for lapses that could not be -- or at least were not -- prevented.

The balance between prevention and detection for depends on the circumstances, and the available security technologies. For example, many homes have easily defeated door and window locks, but rely on a burglar alarm to detect (and signal for help after) intrusions through a compromised window or door.

Most information systems employ a range of intrusion prevention methods, of which user-IDs and passwords are only one part. They also employ detection methods like audit trails to pick up suspicious activity that may signal an intrusion.

Security in context

It is critical to remember that "appropriate" or "adequate" levels of confidentiality, integrity and availability depend on the context, just as does the appropriate balance between prevention and detection.

The nature of the efforts that the information systems support; the natural, technical and human risks to those endeavors; governing legal, professional and customary standards -- all of these will condition how CIA standards are set in a particular situation.

A security question that is (literally) closer to home may be helpful in this regard: Is your personal residence secure? In some situations, simple locks on the doors and closed windows would be enough for a "yes" answer. In others, supplemental deadbolt locks,

high-strength windows, burglar alarms, a vicious dog and a personal weapon would be required for an affirmative response.

What if the same question were asked about the bank where you keep your savings? We suspect your standard for security there would be different than for your home. So it is for information security and CIA: context is (almost) everything.

See also:

National Institute of Standards and Technology - Computer Security Resource Center (NIST-CSRC)
A good overall resource for information security materials

United States Computer Emergency Readiness Team (US-CERT)
Another good overall resource for information security materials

Last modified: 24-Apr-2006 [RC]