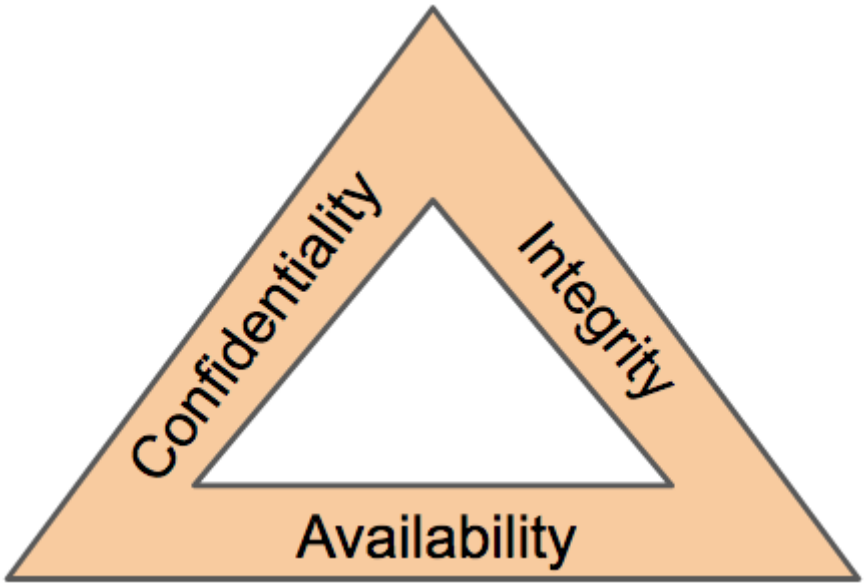
CIA Triad

The CIA triad is an information security model that is used in consideration throughout creating a security policy. This model has an extensive background, ranging from being used in 1998.

This history is because the security of information (information security) does not start and/or end with cybersecurity, but instead, applies to scenarios like filing, record storage, etc.

Consisting of three sections: **C**onfidentiality, **I**ntegrity and **A**vailability (**CIA**), this model has quickly become an industry standard today. This model should help determine the value of data that it applies to, and in turn, the attention it needs from the business.



The CIA triad is unlike a traditional model where you have individual sections; instead, it is a continuous cycle. Whilst the three elements to the CIA triad can arguably overlap, if even just one element is not met, then the other two are rendered useless (similar to the fire triangle). If a security policy does not answer these three sections, it is seldom an effective security policy.

Whilst the three elements to the CIA triad are arguably self-explanatory, let's explore these and contextualise them into cybersecurity.

Confidentiality

This element is the protection of data from unauthorized access and misuse. Organisations will always have some form of sensitive data stored on their systems. To provide confidentiality is to protect this data from parties that it is not intended for.

There are many real-world examples for this, for example, employee records and accounting documents will be considered sensitive. Confidentiality will be provided in the sense that only HR administrators will access employee records, where vetting and tight access controls are in place. Accounting records are less valuable (and therefore less sensitive), so not as stringent access controls would be in place for these documents. Or, for example, governments using a sensitivity classification rating system (top-secret, classified, unclassified)

Integrity

The CIA triad element of integrity is the condition where information is kept accurate and consistent unless authorized changes are made. It is possible for the information to change because of careless access and use, errors in the information system, or unauthorized access and use. In the CIA triad, integrity is maintained when the information remains unchanged during storage, transmission, and usage not involving modification to the information. Steps must be taken to ensure data cannot be altered by unauthorised people (for example, in a breach of confidentiality).

Many defences to ensure integrity can be put in place. Access control and rigorous authentication can help prevent authorized users from making unauthorized changes. Hash verifications and digital signatures can help ensure that transactions are authentic and that files have not been modified or corrupted.

Availability

In order for data to be useful, it must be available and accessible by the user.

The main concern in the CIA triad is that the information should be available when authorised users need to access it.

Availability is very often a key benchmark for an organisation. For example, having 99.99% uptime on their websites or systems (this is laid out in Service Level Agreements). When a system is unavailable, it often results in damage to an organisations reputation and loss of finances. Availability is achieved through a combination of many elements, including:

- Having reliable and well-tested hardware for their information technology servers (i.e. reputable servers)
- Having redundant technology and services in the case of failure of the primary
- Implementing well-versed security protocols to protect technology and services from attack

---

Revision #2
Created 2023-02-11 20:51:35 UTC by Fettlaus
Updated 2023-02-11 21:16:51 UTC by Fettlaus