What is the CIA Triad? Confidentiality, Integrity and Availability

By: ryan c

June 9, 2015

The CIA triad is becoming the standard model for conceptualizing challenges to information security in the 21st century. CIA stands for confidentiality, integrity and availability, which are said to be the three most important elements of reliable security. Every IT worker should have a thorough understanding of the triad and its intricacies, but every staff member who works around sensitive data should at least be made aware of the concept, which is why the concept is a foundation to our Security Awareness Course. The topic also makes appearances in other core classes, such as in the CASP class lessons on CIA.**The Triad**In simple terms, the three parts of the CIA triad can be summarized as follows:

- Confidentiality: Rules limiting who has access to information
- Integrity: Rules governing how and when information is modified
- Availability: Assurance that people who are authorized to access information are able to do so

ConfidentialityConfidentiality is synonymous with privacy. Confidentiality measures prevent data from falling into the hands of people who do not have authorization to access said information. In organizations that store large amounts of information, data may be classified based on how detrimental it would be to the organization in the case of a data breach. This process may help direct development of varying levels of security.Ensuring confidentiality requires that all people who have access to sensitive information understand the risks involved. This is often accomplished in special training sessions and may include a lesson in best practices for password safety and social engineering methods. Not only should these employees know how all of the security measures work, they should be able to identify potential risks and be familiar with the legal ramifications associated with data breaches.Everyday examples of confidentiality measures include bank card pin numbers, routing numbers on checks and email passwords. Two-factor authentication, which means using a combination of confidentiality measures such as a password and finger print identification, is common in the professional world. Other aspects of confidentiality include limiting how many places data is stored and the frequency with which data is transmitted. Air gapped computers, disconnected storage devices and keeping only hard copies of documents are all stronger types of confidentiality measures.**Integrity**In the IT world, integrity is all about making sure information is accurate and always stays that way. Common measures to protect integrity include file permissions and version controls to prevent accidental changes or deletion. Ensuring integrity also requires protection against non-human-related errors such as server crashes. Most importantly, information must be backed up to allow quick recovery when disasters happen.**Availability**Ensuring availability requires routine maintenance and upgrading of hardware, software and operating system environments. Maintaining adequate bandwidth to limit bottlenecks and developing a comprehensive disaster recovery plan, which includes consideration of natural disasters like floods and fires, is also necessary to ensure availability. Firewalls and proxy servers are additional tools that fall under the umbrella of protecting information availability.**New Considerations for the CIA Triad**Big data is presenting new challenges to the CIA model because of the massive amount of information being stored, the many sources from which data originates and the array of formats in which the data is stored. Making duplicate copies of so many documents can get expensive fast, and managing big data requires a lot of staff, which multiplies the risks of security breaches and makes oversight difficult.The Internet of things, which involves the increasing capacity for devices other than computers to connect with the Internet, adds additional challenges: for example, in early 2014, security company Proofpoint uncovered a scheme in which household appliances, including a refrigerator, were being hacked and used to steal data from nearby computers. Any product with a computer chip and the ability to network with other machines is vulnerable, and many appliances, like some smart refrigerators, lack adequate security measures to protect against hackers. All new appliances purchased for use around servers containing sensitive information should be carefully vetted by IT staff.No matter how large or small a business or non-profit is, they all deal with sensitive information to some degree. Since new challenges are emerging faster than ever before, CIA should become part of the standard lexicon in offices across the world.