Nicholas Rossler

Confidentiality, Integrity, and Availability are the three aspects of the CIA triad. The CIA triad is a model that helps guide organizations to properly secure their information. By using the CIA triad to guide policies and procedures in organizations it helps build strong foundational cybersecurity needs.

Confidentiality is the first aspect of the CIA triad. Confidentiality focuses on making sure the right procedures and measures are in place to prevent unauthorized access to sensitive information. This sensitive information can a wide array of information such as trade secrets, personal information, and intellectual property for a few examples. This is important for organizations because if unauthorized entities can get access to sensitive personal information, it can lead to a lack of trust from consumers. By upholding confidentiality, it helps gain and maintain trust because customers can be assured that their private information will be protected from unauthorized access. Confidentiality can be upheld with security measures such as two-factor authentication, and data encryption.

Integrity is the second aspect of the CIA triad. Integrity focuses on "maintaining the consistency, accuracy, and trustworthiness of data over its entire lifecycle" (Chai). Integrity is important because as data and transmitted, senders and receivers of the data want to make sure that it can't be altered by unauthorized people. If Bob was to send data over to Sally, both Bob and Sally would want the data to be unaltered and accurate when it is sent and received. Integrity can be upheld with measures such as checksums, to verify that the information is accurate and unaltered. Having backups and versions of data is also important, if the data is altered by accident, it can be reverted back to a previous version to maintain its correct state.

Availability is the last aspect of the CIA triad. Availability focuses on information being available at all times. Availability is making sure that the data is available for those who are authorized and authenticated to access the data at all times. If systems are to go down and that data is not accessible, it is important to have recovery plans to make sure the data is back online and accessible as quickly as possible.

Many confuse authentication and authorization by not realizing the difference between the two. Authorization controls what a user is allowed to do. This can be file permissions, privileges, or roles that a user has that grants them access to certain information and tools. Authentication on the other hand is the process of confirming the identity of a user. Authentication can be done though measures like a username and password that verifies who the user is. To put this into an example, if Bob was getting to his workplace and logging into his desktop. By putting in his username and password and verifying he is Bob, this would be authentication. He is proving he is indeed Bob accessing his account, authentication happens before signing in. Authorization will happen after he logs in. Once he is logged in, his account will have permissions or roles that determine what he is allowed to access, from software, tools, and information. These permissions that decide what he can do is the authorization.

Sources:

https://drive.google.com/file/d/16BVXR0lZ0dtz71_-jehq0tpjHPTYf5GM/view?pli=1

https://www.geeksforgeeks.org/computer-networks/difference-between-authentication-and-authorization/