A large portion of cybersecurity revolves around The CIA Triad, confidentiality, integrity, and availability. Wesley Chai (2022) breaks down each element into three categories starting with confidentiality. Confidentiality refers to information that is not publicized. This can include encrypting information so only certain users can read the data stored. Integrity is about information remaining precise and unmodified during storage or transit. Tools to ensure integrity include checksums or even digital signatures. Lastly, availability means that systems, applications, and data will be accessible when needed. Implementing backups, redundant systems, and disaster recovery are ways to improve this. All three principles are important when managing cybersecurity risks.

Authentication verifies who a user is while Authorization verifies what they can access. These are two security processes that accomplish different tasks but help keep information safe. An example of authentication would be if someone enters their username and password. Once that is completed, they are who they say they are. Authorization is where an authenticated user can access certain resources. An example of this would be someone accessing their work system(authentication). They will only be able to read or change certain files based on their authorization.

Chai, W. (2022, June 28). *What is the CIA Triad? Definition, Explanation, Examples.*