Alissia Metcalfe

CYSE 200T

The CIA Triad

The CIA triad is a model designed to guide information security policies within organizations and businesses. Beginning with **confidentiality**, only allowing access to authorized personnel to modify or view data. For example, the SIPRNet (secret internet protocol router network) only authorized personnel with secret clearance and a SIPRNet token may access this network. Then there is **integrity** which is maintaining the authenticity of data. Ensuring data is not being modified within transit and taking proper preventative actions to ensure it isn't modified by unauthorized users. Forms of preventative actions can include data encryption and hashing. **Availability** means ensuring timely and reliable access to and use of information (NIST, 2020). Meaning that systems/ services are always accessible. An example would be the Verizon outage that took place in January 2026. The outage enabled users from accessing cellular data. When comparing authentication to authorization there are two functions that differentiate the two, **who** and **what.** Authentication is the who, it verifies the identity of who the user is. While authorization is

what the user can and cannot access. An example of authentication is two-factor authentication (2FA). This process requires two distinct forms of identification to access an account. An example of authorization is Canvas, students only have access to view and submit assignments while professors have access to view all submitted assignments, grade, and upload to their course work.

References

National Cybersecurity Centre of Excellence NIST (Dec 2020)

Data Integrity: Detecting and Responding to Ransomware and other Destructive Events

Https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html