Confidentiality, integrity, and availability are the key characteristics of the CIA triangle, a foundational model in network security. Each component plays a critical role in securing data and maintaining a secure and functional network environment.

Confidentiality refers to the safeguarding of data against unauthorized access. This approach ensures that sensitive information is only available to those with correct credentials. Techniques such as encryption, access controls, and authentication systems are often used to enforce confidentiality. For example, encrypting connection between clients and servers prevents attackers from intercepting readable data (Stallings & Brown, 2018). In today's digital landscape, when hacks are becoming widespread, maintaining secrecy is crucial to securing personal, corporate, and governmental data.

Integrity assures that data remains correct and unaffected during storage, transport, or processing. When integrity is breached, data may be tampered with, either accidentally or maliciously. Checksums, hash functions, and digital signatures are extensively used to verify that data has not been modified without consent. A single breach of data integrity can lead to financial loss, reputational damage, or incorrect decision-making, especially in areas such as banking or healthcare (Pfleeger & Pfleeger, 2015).

Availability guarantees that authorized users have access to data and network services when needed. This idea involves creating systems that can resist denial-of-service (DoS) attacks, hardware breakdowns, or natural calamities. Load balancing, redundancy, and regular system updates are examples of measures used to assure availability. If availability is compromised, important operations may be delayed or halted, harming productivity and user trust.

While all three criteria are necessary, **availability** should be given the highest consideration throughout network design. Even if data is kept secure and unaltered, it is useless if it cannot be accessed when needed. In areas such as healthcare, finance, or emergency services, system downtime can have catastrophic effects. Therefore, a well-designed network must prioritize uptime, resilience, and disaster recovery. High availability guarantees that enterprises maintain continuity and meet service-level agreements (SLAs).

Moreover, promoting availability does not mean compromising confidentiality and integrity. Instead, it entails designing a balanced security architecture where systems stay operational even under assault or during failure. For instance, using intrusion detection systems, firewalls, and backup power sources all support availability while complementing the other criteria.

In conclusion, confidentiality, integrity, and availability are all interrelated and vital to network security. However, placing attention to availability means that users can rely on ongoing access to secure and accurate data, making it the foundation of a robust and responsive network design.

References:

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in Computing* (5th ed.). Pearson. https://www.pearson.com/en-us/subject-catalog/p/security-in-computing/P200000009559/9780138230746?srsltid=AfmBOooj30ofvMFRamiLVQVFkhskpEpPp7h6ZEXD8dC2C5qvJ9K0FkXP

Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice* (4th ed.). Pearson. https://www.pearson.com/en-us/subject-catalog/p/computer-security-principles-and-practice/P200000003493/9780137502875?srsltid=AfmBOoomBTB84Ee_HTsqzqHugzVSQvQvywFy8dtxbjY3_rqsmq9bjd2E

Wordcount: 408