The CIA Triad: Protecting Confidentiality, Integrity, and Availability in Cybersecurity

Shayla Harmon

Old Dominion University

CYSE 200T

Charlie Kirkpatrick

September 6, 2026

The CIA Triad: Protecting Confidentiality, Integrity, and Availability in Cybersecurity

The CIA triad is an important part of cybersecurity because confidentiality, integrity, and availability work together to protect an organization's information and systems. Failing in any one of these areas can result in data exposure, inaccurate or altered information, system disruptions, financial loss, and damage to an organization's reputation. The 2021 Colonial Pipeline ransomware attack demonstrates how a cybersecurity incident can affect not only an organization but also the people and communities that depend on its services. Organizations can reduce these risks by using security controls such as access controls, muti-factor authentication, system monitoring, and disaster recovery planning.

Confidentiality

In my opinion, confidentiality means making sure that information is only available to people who are authorized to access it. This is especially important when organizations handle and store sensitive information such as passwords, financial information, student records, or personally identifying information. According to Chai (2022), confidentiality is focused on preventing unauthorized access to information and protecting privacy. If an organization does not properly protect confidential information, attackers may be able to access or steal it.

Confidentiality is important to cybersecurity because organizations need to control who can view or use their information. Security practices such as strong passwords, muti-factor authentication, and access controls and help prevent unauthorized access. Employee training is also important because social engineering attacks and trick employees into providing information to attackers (Chai, 2022). Protecting confidentiality can help organizations maintain trust, avoid financial losses, and reduce the potential impact of a data breach.

Integrity

Integrity means making sure that information remains accurate, complete, and trustworthy. Information can lose its integrity when someone changes it without authorization, whether intentionally or accidentally. For example, if an attacker altered information in an organization's database, the organization could make decisions based on incorrect information.

Integrity is important because organizations depend on accurate information to operate effectively. Chai (2022) explains that integrity involves maintaining the consistency and accuracy of information throughout its lifecycle. Security controls such as access permissions or role-based access controls can help protect information from unauthorized changes. Maintaining integrity is especially important for organizations that depend on databases and other information systems to make decisions and conduct daily operations.

Availability

Availability means making sure that authorized users can access systems and information when they need them. Information may be secure from unauthorized users, but it is not useful if authorized users cannot access it. For example, if ODU's student information system goes offline during registration, students will not be able to register for the classes within their registering period.

Availability is an important part of cybersecurity because organizations depend on technology to perform their daily operations. According to Chai (2022), organizations can improve availability through hardware maintenance, system updates, redundancy, failover systems, backups, and disaster recovery plans. These practices can help organizations continue operating when systems experience failures or cyberattacks. Maintaining availability also

requires organizations to monitor their systems and have and have plans for recovering from disruptions.

Real World Example: Colonial Pipeline

The 2021 Colonial Pipeline ransomware attack is an example of how a cybersecurity incident can affect availability and operations. In May 2021, threat actors deployed ransomware against Colonial Pipeline's secure network. In response, the company disconnected certain systems used to monitor and control its physical pipeline operations, which resulted in a temporary halt to pipeline operations (U.S. Government Accountability Office [GAO], 2021). The temporary shutdown disrupted the delivery of gasoline and petroleum products across parts of the southeastern United States. This attack demonstrates how a cybersecurity incident involving one organization can affect individuals, businesses, and other organizations that depend on its services and shows the relationship between the CIA triad.

Reducing the Risk of Similar Incidents

Organizations can use several cybersecurity practices to reduce the likelihood of similar events. One important strategy is to implement strong access controls so that users only have access to the systems and information necessary for their job. Multi-factor authentication can provide another layer of protection if an attacker obtains a user's password. In addition, organizations should also monitor operating systems to reduce vulnerabilities that attacks could exploit.

Risk assessments are also important because organizations need to identify vulnerabilities before they become major problems. Security teams can use risk assessments to determine which threats are most likely to affect the organization and which systems require the most protection.

Regular monitoring, employee security training, and security assessments can further strengthen an organization's overall security stance.

Conclusion

The CIA triad provides a foundation for understanding and applying cybersecurity practices. Confidentiality in the CIA triad, keeps information protected from people who should not have access to it, integrity makes sure information stays accurate, whereas availability ensures authorized users can access the information and systems when they need them. These principles depend on each other and failure in one area can cause serious issues. The Colonial Pipeline ransomware attack demonstrates how a cybersecurity incident can disrupt an organization and affect individuals beyond the business itself. By using security controls, conducting risk assessments, monitoring systems, and preparing recovery plans, organizations can better protect their information and continue operating when threats occur.

References

Chai, W. (2022, June 28). *What is the CIA triad? Definition, explanation, examples*. TechTarget.

U.S. Government Accountability Office. (2021, July 27). *Critical infrastructure protection: TSA is taking steps to address some pipeline security program weaknesses* (GAO-21-105263).