

Tracey Bernasco

CYSE200T_15188

The CIA Triad

Importance of CIA Triad and real-world Applications

Cybersecurity's main goal is to protect the information and systems that organizations rely on every day. One framework used to understand cybersecurity is the CIA triad which consists of confidentiality, integrity and availability. In this paper we will examine the CIA triad and analyze how this cybersecurity principle can be applied to real-world security incidents.

Confidentiality is the process in which information is only accessible for people or systems that are authorized to use it. It is an important part of cybersecurity because organizations must store large amounts of sensitive information such as client's information, passwords and business data. This component of the CIA triad is important to cybersecurity practices because without confidentiality, attackers could gain access to sensitive information that could lead to data breaches. One such major incident that involved the failure of confidentiality is the 2017 Equifax data breach. Cyber criminals accessed data such as social security numbers, birthdates and addresses. This attack happened as the hacker's had unauthorized access to its system by exploiting a website application vulnerability. (BBC, 2017) This impact has affected millions of people, and this type of information cannot be changed, and it is a financial burden as well. Several cybersecurity practices that could help reduce the likelihood and impact similar incidents in the future would be to regularly identify and patch known software vulnerabilities. Implementing encryption, multi-factor authentication and continuous security monitoring as well as regular vulnerabilities assessments to better protect the sensitive data. One way that organizations should also implement is the incident response plan so

that security breaches can be detected and contained quickly as possible. These practices can reduce unauthorized access and help protect sensitive information.

Integrity is about maintaining the information that stays accurate and trustworthy unchanged unless someone who is authorized can change as well as preventing unauthorized people from changing or manipulating it. This is essential to cybersecurity because organizations must be able to trust the information they use has not been compromised and changed by unauthorized individuals. If the data is changed to be inaccurate this could lead to financial losses, and operation disruptions that could damage the organization's reputation. A real-world example would be the 2020 SolarWinds cyberattack. Attackers were able to access SolarWinds's software development and insert malicious code into legitimate software updates that were distributed to customers, because that attacks were able to compromise the integrity of the software it affects numerous organizations, and even government agencies. Sophisticated supply chain attacks often exploit the inherent trust placed in automated updates and third-party monitoring exclusions to bypass traditional perimeter security and Endpoint Detection and Response (EDR) tools (Datta, 2022). This incident demonstrated how comprising the integrity of trusted software can create widespread cybersecurity risks because organizations may unknowingly install malicious code.

Availability means ensuring that authorized users can access information when needed without unnecessary interruptions or downtime. Availability is important to cybersecurity farmwork because organizations depend on technology to perform daily operations. A real-world example of the failure of this would be the July 2024 CrowdStrike-Microsoft Windows outage. CrowdStrike released a content configuration update for Windows systems that contained a defect. The update caused Window computers to crash and display the "Blue screen of death"

that prevented many systems from operating normally. System availability can be compromised not only by malicious cyberattacks but also by updates in security software supply chains, as demonstrated when a single faulty agent update rendered approximately 8.5 million endpoints unavailable (Weston, 2024). Unlike some of the other examples, this was not a cyber-attack.

While there are examples involving cyberattacks like ransomware, I wanted to use this example as with cybersecurity it is not only important to be aware of the cyber vulnerabilities but as well as the operational availability. The outage had significant impact on individuals and organizations all over the world, including healthcare, banks and anyone who used Windows-based systems. It is important to thoroughly test software updates before widespread deployment and maintain backup system and developing disaster recovery and business continuity plans. These practices can improve system availability and help organizations continue operations when unexpected technical incidents occur.

Authentication and authorization work together to control access to system and information. Authentication is the process of verifying a user's identity before granting access to an account or system, examples of this include passwords, fingerprints, multifactor authentications. Authorization on the other hand determines what authenticated user is allowed access within a system. This would be if an employee who needs to be authenticated to access a company's network but only authorized to view specified files based on their job. The main difference is that authentication determines who the user is while the authorization determines what the user is allowed to do. Both processes are important as they help organizations prevent unauthorized access and protect sensitive information.

In conclusion, the CIA triad provides an important foundation for understanding and practicing cybersecurity. Each framework helps protect sensitive information from unauthorized

access, with integrity to ensure information remains accurate and having systems maintain availability. Each example shows how failures significantly impact not only individuals but organizations. These show the importance of implementing strong security practices and help reduce potential impact of future cybersecurity incidents.

References

- BBC, *Massive Equifax data breach hits 143 million*, Sept. 7 2017, <https://www.bbc.com/news/business-41192163>
- Datta, P. (2022). Hannibal at the gates: Cyberwarfare & the Solarwinds sunburst hack. *Journal of Information Technology Teaching Cases*, 12(2), 115–120. <https://doi.org/10.1177/2043886921993126>
- Weston, D. (2024, July 20). *Helping our customers through the CrowdStrike outage*. The Official Microsoft Blog. <https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/>