The CIA Triad:

The Three Pillars of the CIA Triad

Andrew Judy

School of Cybersecurity, Old Dominion University

CYSE/IT 200T - Cybersecurity, Technology, & Society

Professor Chris Bowman

September 6, 2026

The CIA Triad, which stands for confidentiality, integrity, and availability, is the model that is used to guide policies properly secure and safeguard the information of an organization. All three pillars of the triad share equal importance to each other; as they play a vital role in ensuring proper cybersecurity within the organization. This paper will explore each of the pillars, why each pillar is important, provide an example of one of these pillars coming under attack in a past incident, the impact this incident had, provide possible solutions and remedies to help prevent future incidents in all three pillars, and define authentication versus authorization.

Authentication is the act of confirming the identification of the user they claim to be. A common example of authentication in-practice is a password, which serves as a layer of verification to confirm or deny the identity that the user claims to be. Another example of authentication includes multi-factor authentication; MFA for short. Multi-factor authentication includes passwords in addition to another layer of verification required to more thoroughly confirm the identity of the user. This additional layer, for example, can include a prompt to type in a randomized letter and/or number code that is sent to a different device, such as a phone or a computer, when the user passes the initial authentication layer of using the correct password. Authorization, on the other hand, is the set of rules and permissions that are given to an authenticated user once the user's identity is verified. This includes giving permission to said user to access data and information within an organization to an extent that is deemed appropriate and necessary by the organization. To expand on, for example, new employees hired at a company will likely have minimal access if any to certain information because trust must be earned between the new employee and company in order to have the permission to access data that are more or less confidential. Once trust is built, however, authorization may be expanded to the authenticated user to allow them to access more confidential data.

Confidentiality can be defined as keeping sensitive information secure by implementing multiple security layers to lower the risk of a potential breach in security. In the real world, for example, actions such as implementing two-factor authentication and biometric scans for login prompts serve to improve confidentiality and bolster cybersecurity. Therefore, it is important to maintain organizational security and use cybersecurity practices such as these. Leaving this sensitive information unprotected can cause a plethora of issues for the individuals who are storing information within these systems of the organization, and the damage that can be caused by an individual who gains access to such information can be catastrophic for both the organization and the individual. An action that individuals and organizations can take to help reduce risk to possible breaches and mitigate potential damage could include strengthening security parameters such as implementing multi-factor authentication to potentially discourage inexperienced individuals such as script kiddies from attempting to gain unauthorized access to sensitive information. Another possible precaution individuals and organizations alike can partake in is educating other individuals or organizations on the importance of taking actions to keep information such as social security numbers or passwords from falling into the wrong hands, sharing sensitive information with no-one, and storing confidential information only in systems that contain sophisticated security layers, such as systems that contain multi-factor authentication.

Integrity involves ensuring that information is kept the exact same and is not altered unless done so by an authorized individual. This includes ensuring that data is not changed at rest or in transit from individual to system, or vice versa, and that data cannot be altered by unauthorized individuals. An example of a failure of integrity happening in real life would be the SolarWinds Supply Chain cyberattack, which began in September 2019 and lasted until

December 2020. According to Fortinet, a cybersecurity and networking company, they report that an estimated 18,000 SolarWinds customers installed updates that contained malicious code. As a result, the impacts from this cyberattack were substantial. Fortinet goes on to say: “The attack cost companies 11% of their annual revenue. The impact was more dramatic in the United States than across the seas. In the U.S., the average impact was 14% of annual revenue, while U.K. companies suffered 8.6% losses” (Fortinet, n.d.). This illustrates the economic impact that this attack had on companies in different parts of the world. An action that organizations can take to ensure integrity would be to implement multi-factor authentication, which would create an additional layer of verification to deny unauthorized changes to data, regardless of whether or not the data is at rest or in transit. Another measure that can be taken would be to enable automatic updates, which would ensure that operating systems and software alike are patched to inhibit an attacker’s ability to potentially exploit any known weaknesses.

Availability means that information should be able to be accessed at any given time by an authorized individual for use. Ensuring that this pillar is present in any organization for users is crucial because individuals may need to access sensitive information at any given time for various reasons, such as transferring money to a different account, paying financial expenses, or making a deposit. If such systems are not protected, threats can potentially disrupt such systems by using attack methods such as a DDoS attack (Distributed-Denial-of-Service) to overload systems with large amounts of data to prevent normal data traffic from occurring and bringing servers hosting these systems to a halt. Actions that can be taken to mitigate and lower the risk of a DDoS attack from happening can include improving infrastructure by forcing traffic to go through a cloud-based security platform to filter out potentially malicious traffic, and being on the lookout for malicious traffic by monitoring network traffic consistently and effectively. By

taking these actions, availability can be achieved for users to allow them to access whatever information they need for whenever they need to.

The CIA Triad consists of confidentiality, integrity, and availability. This paper serves to explain what the CIA Triad is, its importance in the real world for individuals and organizations alike, provide examples of its pillars, and explore remedies that individuals and organizations can take to secure all three pillars and ensure the total effectiveness of each. By practicing each pillar of the CIA Triad effectively, individuals and organizations contribute to the promotion of effective cybersecurity practices in cyberspace.

References

Fortinet, (n.d.). *SolarWinds supply chain attack*.

https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack