

The CIA Triad

—

Pillars of Cybersecurity & Their Application

Jayden Dorey

CYSE 200T

Professor Kirkpatrick

6 September 2026

Definitions

The CIA triad – not to be confused with the Central Intelligence Agency – is the model used to explain the pillars of cybersecurity and information security practices. Some refer to it as the AIC triad to avoid this confusion. Either way, the acronym represents Confidentiality, Integrity, and Availability, and describes the relationship they share to uphold information security.

Confidentiality explains who has the ability to access the information and, more importantly, guaranteeing no one can access it except those that do have access (Kim & Solomon, 2023, 13).

Integrity defines the validity and accuracy of information, ensuring no unauthorized edits have been made to taint data (Kim & Solomon, 2023, 13).

Availability covers the idea of being able to access information when necessary and can be calculated using a mathematical formula, which describes the relationship between uptime and downtime for systems that house the data (Kim & Solomon, 2023, 13).

Authentication vs. Authorization

Despite similar spelling, authorization and authentication are two different terms. Authentication describes the process of proving a user is who they say they are by providing a key or keys (Kim & Solomon, 2023, 34). These keys are usually something you know, like a password, something you have, like a badge or RFID key, and something you are, like a biometric (e.g. fingerprint, retina, facial recognition). On the other hand, authorization is the process of giving someone permission or rights to access (Kim & Solomon, 2023, 13).

It is helpful to think of them as logical steps, where one first needs to be granted authorization in order to go through the authentication process.

Application

In 2024, National Public Data fell victim to a threat actor that exfiltrated approximately 2.9 billion PII records of individuals from the United States, Canada, and the United Kingdom (Gregory, 2024). During this attack, the threat actor was able to gain unauthorized access to the company's internal network, which housed their database. NPD was a background check service provider, meaning their database was filled with full names, social security numbers, and other sensitive personal information. After the initial intrusion in December 2024 and months of quietly exfiltrating this data, a threat actor under the alias "USDoD" advertised the dataset for sale on the dark web for \$3.5 million in April 2024 (DeXpose, 2025). This data did not stay in their sole possession for very long. In August of 2024, another threat actor under the name "Petrovic" released a portion of the data set to a public hacking forum, and a few days later, an additional actor, "Fenice", released the rest of the data set, exposing all 2.9 billion records to the public (DeXpose, 2025).

This attack demonstrates the exploitation of the **confidentiality** pillar of the CIA triad. The threat actor was not authorized to access the internal network, corrupting the confidentiality that the company was expected to have between them and their customers.

Analysis & Impact

National Public Data faced extreme public backlash for their entire attitude and strategy while handling the attack. The company chose not to give a public statement until the threat was confirmed in August of 2024. Legally, they were fine because they are not governed by CIRCIA, so they are not mandated to release a statement following the normal 24-72 hour regulation (CISA, n.d.). However, this was not deemed widely acceptable by those impacted. As a result, many class action lawsuits have been filed against the company. Even still, the company seemed

to escape those penalties by filing for bankruptcy under Chapter 11 (DeXpose, 2025). Because of this, the courts have not ruled on an amount to be paid out to the plaintiffs because the assets of the companies have not been determined to be able to cover the costs.

Strategy

In terms of security standards, a simple modification could have mitigated this situation. The attack was successful because the threat actor was able to gain unauthorized access to their network, which also held their database. A VLAN could have made it more difficult for the actor to gain access to their internal database. By segmenting a network, a company can mitigate one attacker gaining access to everything owned by the company. If the actor was able to infiltrate the primary network, they still would not have been able to access the network housing the database. In order to prevent the actor from gaining access to the main network, a more robust IDS or IPS could have been used. Alternatively, NDP could have been more dutiful with their access control list. One of the ways to ensure confidentiality is upheld, according to Welsey Chai, is to “keep access control lists and other file permissions up to date” (Chai, 2022). Doing so may have given their IDS time to detect a threat actor attempting to gain access to their network.

Conclusion

The CIA triad exists as a guideline to help focus the security efforts across the variety of fields that use technology. Maintaining confidentiality, integrity, and availability is crucial to any company that handles data and information of any kind. As seen in the National Public Data Breach of 2024, simple security flaws pertaining to the CIA triad can have major and lasting consequences to both the organization and their customers.

References

- Chai, W. (2022, June 28). *What is the CIA Triad? Definition, Explanation, Examples*. TechTarget. <https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA?jr=on>
- CISA. (n.d.). *CIRCIA FAQs*. Cybersecurity & Infrastructure Security Agency. <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/circia/faqs>
- DeXpose. (2025, August 6). *National Public Data Breach | What Happened, Who's Affected & How To Check Your SSN*. DeXpose. <https://www.dexpose.io/national-public-data-breach/>
- Gregory, J. (2024, August 19). *National Public Data breach publishes private data of 2.9B U.S. citizens*. IBM. <https://www.ibm.com/think/news/national-public-data-breach-publishes-private-data-billions-us-citizens>
- Kim, D., & Solomon, M. G. (2023). *Fundamentals of Information Systems Security* (Fourth ed.). Jones & Barlett Learning. <https://reader2.yuzu.com/reader/books/9781284238815>