



TUESDAY – DAY 2

The CIA Triad & Core Security Principles

Confidentiality, Integrity, Availability

Facilitator Teaching Guide – Cybersecurity Track, Week 1
Prepared for Kelechi Nkwocha, Cybersecurity Track Facilitator

1. Learning Objectives

By the end of this session, students should be able to define confidentiality, integrity, and availability, explain how these three principles interact and sometimes conflict, and apply the CIA triad to evaluate a real-world security scenario.

2. What Is the CIA Triad?

The CIA triad, confidentiality, integrity, and availability, is the foundational model of information security. It is not a specific technology or tool; it is a way of thinking that helps security professionals evaluate whether a system is genuinely protected. Every control taught for the rest of this course, from firewalls to access policies to incident response, exists to serve one or more of these three goals.

Facilitator note

Emphasize early that a system is only as secure as its weakest pillar. A system can have perfect confidentiality, data locked away so tightly no one can read it, and still be a complete security failure if that also means legitimate users cannot access it when they need to. The three pillars must be balanced, not maximized individually.

3. Confidentiality

Confidentiality means ensuring that information is accessible only to those authorized to see it. It is roughly equivalent to privacy. Data is typically classified by sensitivity, public, internal, confidential, restricted, and protected accordingly.

How confidentiality is enforced

- Encryption — scrambling data so it is unreadable without the correct decryption key, both at rest (stored data) and in transit (data moving across a network).
- Access controls — usernames, passwords, and permission systems that restrict who can view specific data.
- Authentication — verifying that a user is who they claim to be, increasingly through multi-factor authentication.

Real-world example: when a bank encrypts customer account data and only allows tellers to view the accounts assigned to their branch, that is confidentiality in action. A breach of confidentiality is what happens in a typical data leak, customer records, medical files, or trade secrets exposed to people who should never have seen them.

4. Integrity

Integrity means ensuring that data is accurate, complete, and has not been tampered with, whether by accident or by a malicious actor, at any point in its lifecycle.

How integrity is enforced

- Hashing — generating a unique digital fingerprint of a file; if the file changes even slightly, the hash changes, revealing tampering.

- Digital signatures — cryptographically proving that a piece of data came from a specific source and was not altered in transit.
- Change management and version control — formal processes that track who changed what, and when, in a system.

Real-world example: if an attacker intercepts a bank transfer instruction and changes the destination account number, that is an integrity violation, the data was altered without authorization. Integrity is also why software downloads often list a checksum you can verify before installing.

5. Availability

Availability means ensuring that systems and data are accessible to authorized users whenever they are needed. Security that locks legitimate users out is a failure of availability, even if confidentiality and integrity are perfectly intact.

How availability is enforced

- Redundancy — backup systems, servers, and power supplies that keep services running if one component fails.
- Regular backups — so data can be restored quickly after an outage, hardware failure, or ransomware attack.
- DDoS protection — defenses against distributed denial-of-service attacks, where attackers flood a system with traffic to knock it offline.

Real-world example: a ransomware attack that encrypts a hospital's patient record system is fundamentally an availability attack. The data may still be perfectly intact and confidential; the harm is that authorized staff can no longer access it when a patient needs care.

6. The Tension Between the Three Pillars

A key teaching point: the three pillars often pull against each other, and good security design is about finding the right balance for the context, not maximizing all three blindly.

- More confidentiality (more locks, more approval steps) can reduce availability by making access slower or harder for legitimate users.
- More availability (open access, minimal friction) can reduce confidentiality by making it easier for the wrong people to get in too.
- The right balance depends entirely on context: a hospital's emergency system may prioritize availability above all else, while a national defense database may prioritize confidentiality even at some cost to convenience.

7. Applying the Triad: A Classroom Exercise

Present this scenario to the class and ask them to identify which pillar (or pillars) is being violated in each case:

- A disgruntled employee copies a customer database onto a USB drive before resigning. (Confidentiality)
- A server room floods and the company's only backup is destroyed along with the primary servers. (Availability)
- A hacker changes the grades in a university's student records system. (Integrity)
- A company's website is knocked offline for six hours by a flood of fake traffic. (Availability)

- An attacker gains access to a hospital database and quietly alters patient blood type records. (Integrity, with dangerous real-world consequences)

8. Key Terms Introduced Today

- Confidentiality – ensuring information is only accessible to authorized parties.
- Integrity – ensuring data is accurate and has not been improperly altered.
- Availability – ensuring systems and data are accessible to authorized users when needed.
- Encryption, hashing, redundancy – core technical mechanisms supporting each pillar respectively.

9. Looking Ahead

Wednesday's session builds directly on this foundation by exploring specific threat types, malware, phishing, social engineering, and insider threats, and framing each one in terms of which pillar of the CIA triad it primarily attacks. Encourage students to start thinking in these terms now.