

Information Security Foundations: Confidentiality, Integrity, and Availability

- Information security protects data and systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- The CIA triad is the central model: Confidentiality, Integrity, and Availability.
- A shared vocabulary bridges gaps between technical and business teams when discussing risk.
- This session covers each CIA element, how they interact, trade-offs, and applying the vocabulary.



Why the CIA Triad Matters to You

- A simple checklist for evaluating security in any situation
- A shared vocabulary bridging technical and business teams
- Security is a business enabler, not just an IT problem
- Every employee plays a role in protecting CIA



What Is Confidentiality?



Confidentiality: preventing unauthorized disclosure of information



Data at rest (stored), in transit (emails), and in use (active)



Core controls: encryption, access controls, authentication, labels



Everyday examples: locked cabinets, passwords, private messaging



Data at rest
(stored)



Data in transit
(emails)



Data in use
(active)

Confidentiality in the Real World

- The Change Healthcare attack exposed health data of over 100 million individuals
- Stolen data included diagnoses, SSNs, and financial details, risking identity theft
- Breach origin: stolen credentials used on a system without multi-factor authentication
- Best practices: use strong passwords, enable MFA, and lock screens when away
- Ask "who should have access?" before sharing any document



What Is Integrity?



- Ensuring data is not improperly modified, deleted, or corrupted



- Accidental changes: hardware errors, human mistakes



- Malicious changes: tampering, ransomware attacks



- Key controls: hashing, checksums, version control, audit logs, digital signatures



- Real-world: tamper-evident seals, bank reconciliation, read-only permissions



Integrity Failures and Their Impact

- Change Healthcare: ransomware corrupted critical healthcare data
- Snowflake attacks (2024): stolen credentials enabled potential data tampering
- Verify data before acting; use version history for key documents
- Report unexpected changes immediately
- Integrity is trust—compromised data means compromised decisions



What Is Availability?

- “Availability ensures timely, reliable access to information and systems”
- “Distinguish planned downtime (maintenance) from unplanned outages (attacks, disasters)”
- “Basic controls: redundancy, backups, disaster recovery, and DDoS protection”
- “Relatable examples: cloud sync, hospital generators, e-commerce uptime”



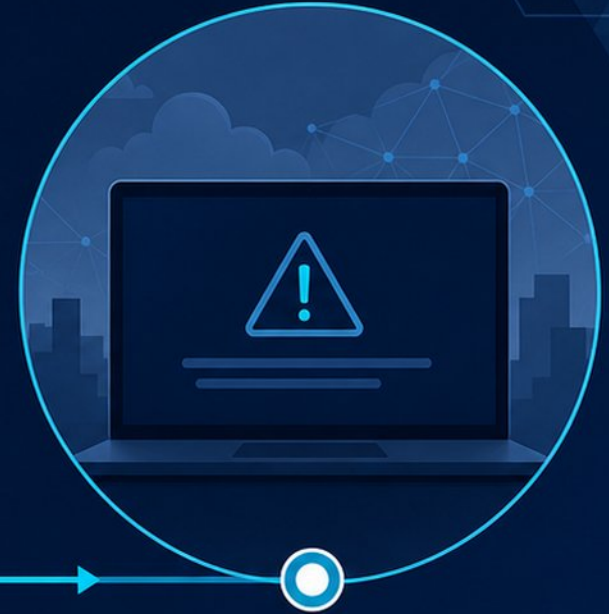
When Availability Is Lost



Change Healthcare outage: insurance claims, pharmacy transactions halted nationwide



Internet Archive suffered DDoS and data breach simultaneously in 2024



Know backup procedures, report outages immediately, have offline alternatives



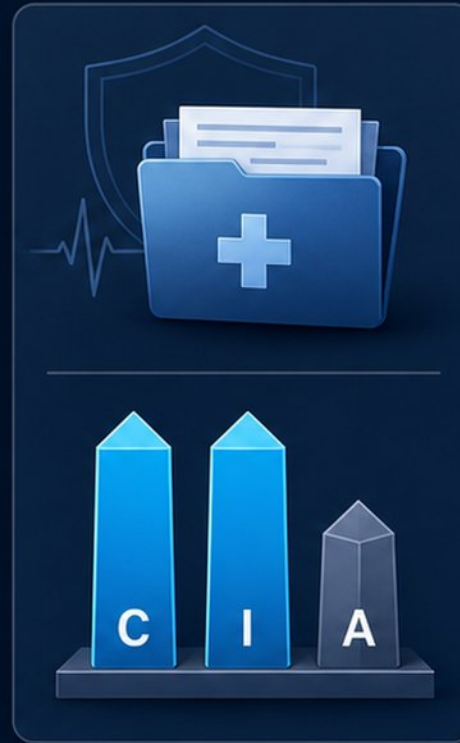
Availability is the ability to perform your job functions, not just uptime

The CIA Triad in Practice: Trade-Offs



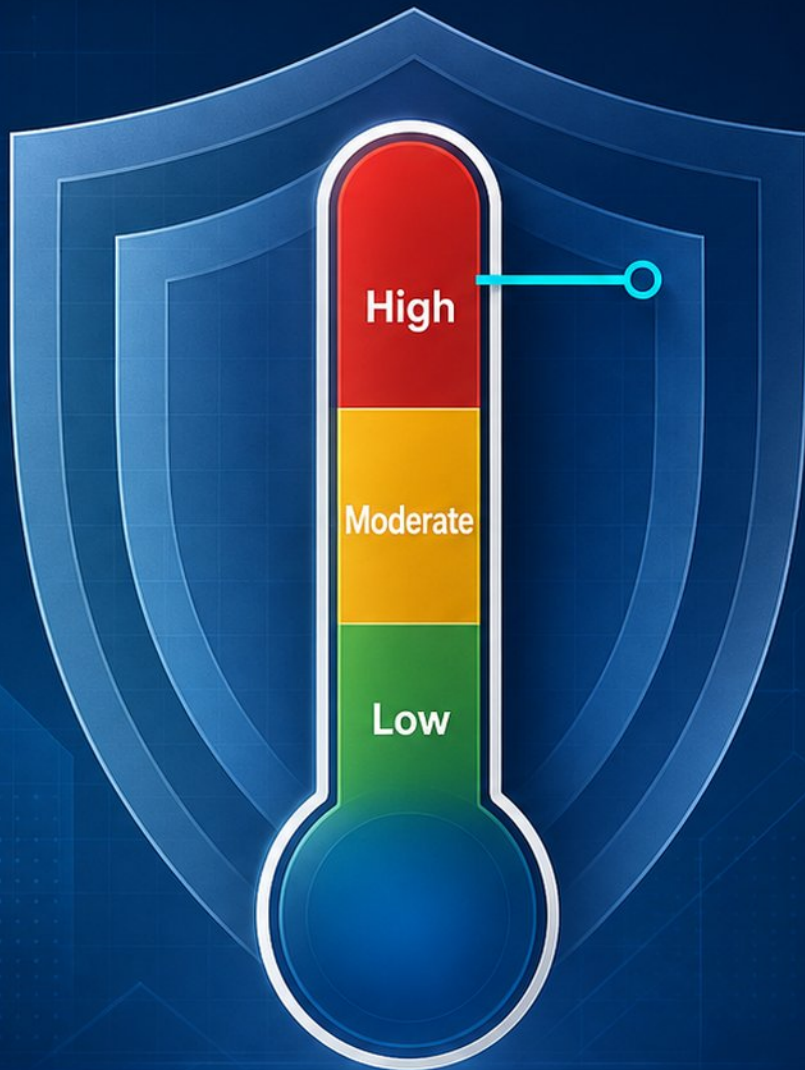
- Security goals often conflict; strengthening one can weaken another.
- Stronger encryption (confidentiality) can slow access (availability).
- Always-on access (availability) may reduce authentication steps (confidentiality).
- Balance CIA goals based on business context and risk appetite.

Identifying CIA Priorities for Different Assets



- Public website: Low Confidentiality, High Integrity, High Availability
- Payroll database: High Confidentiality, High Integrity, Moderate Availability
- Medical records: High Confidentiality, High Integrity, Moderate Availability
- Source code: High Confidentiality, High Integrity, Moderate Availability
- Same organization, different CIA profiles per data type

Understanding Impact Levels



- **Low:** Limited adverse effect; minor mission degradation or financial loss
- **Moderate:** Serious adverse effect; significant degradation or financial loss
- **High:** Severe/catastrophic effect; mission loss or major financial loss
- **High water mark:** overall system impact level is the highest among C, I, A

Common Terminology Beyond the Triad



Authentication:

proving your identity (e.g., password, fingerprint)



Authorization:

defining what you are allowed to access



Non-repudiation:

preventing denial of an action (e.g., digital signature)



Privacy:

controlling how personal data is collected and used

> These concepts support and extend the CIA triad in practice



Applying the CIA Vocabulary

Use CIA terms to describe security concerns clearly

Scenario:

A phishing email captures a password (Confidentiality)



Scenario:

A hard drive fails without a backup (Availability)



Raise concerns in meetings with CIA language



Shared vocabulary bridges technical and business teams

Summary and Key Takeaways



- The CIA triad: Confidentiality, Integrity, Availability



- Security balances these three goals—trade-offs are normal



- Ask: Is it confidential?
Is it accurate?
Is it available?



- Use the one-page reference card with definitions and impact levels



PersonWise.

PersonWise • AI digital-human course platform



Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/5819fad9/public