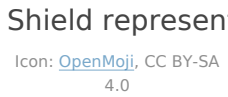
Cybersecurity and the CIA triad

Threats, vulnerabilities and risks



Shield represen

Icon: OpenMoji, CC BY-SA 4.0

Cybersecurity protects digital systems, networks and data from harm. The harm may be deliberate, such as stealing records, or accidental, such as deleting a shared file. A power failure, faulty update or overloaded server can also create a security problem.

To investigate a scenario, separate three ideas:

- **Threat:** something that could cause harm, such as an attacker, fire or careless user.
- **Vulnerability:** a weakness that could be exploited, such as a shared password or missing backup.
- **Risk:** the possibility that a threat exploits a vulnerability and causes a consequence.

Spot the threat, weakness and risk

A club stores its membership database on one unprotected laptop. Match each item to *threat*, *vulnerability* or *risk*.

1. The laptop is stolen.
2. The laptop has no sign-in protection or encrypted storage.
3. An unauthorised person may read members' addresses.

Check your answer

1. **Threat:** theft of the laptop could cause harm.
2. **Vulnerability:** the missing protections make access easier.
3. **Risk:** private data may be disclosed, causing harm to members.

Confidentiality, integrity and availability

In cybersecurity, the CIA triad identifies three properties that data and systems should preserve.

Property	The question to ask	A compromise
Confidentiality	Can only authorised people access the data?	A stranger views private medical results.
Integrity	Is the data accurate, complete and protected from unauthorised change?	A price is accidentally changed from $25 to $2.
Availability	Can authorised users access the data or service when needed?	A booking system is offline during enrolment.

> **Key idea:** Authorised access matters. Keeping everyone out would preserve secrecy, but a system that legitimate users cannot access has poor availability.

Classifying a compromise

- **Who saw it?** Think confidentiality.
- **Who or what changed it?** Think integrity.
- **Could the right person use it at the right time?** Think availability.

Check for understanding

Determine the main CIA property compromised in each incident.

1. A student changes another student's attendance record.
2. A flood damages the only server holding assessment files.
3. A spreadsheet containing home addresses is emailed to the wrong group.
4. A surge of traffic prevents customers from opening an online store.

Check your answer

1. **Integrity:** the record has been changed without authorisation.
2. **Availability:** authorised users cannot retrieve the only stored copy.
3. **Confidentiality:** unauthorised recipients can view personal data.
4. **Availability:** legitimate customers cannot access the service.

Constructing a risk analysis

Writing “confidentiality risk” names a category but does not show the reasoning. Build a short chain that connects evidence to a consequence.

> **Because** [scenario evidence], [threat or event] could [what happens to the data or service], **which compromises** [CIA property] **because** [consequence for an authorised user, person or organisation].

Worked example

A sports club lets every volunteer use the same administrator account to view and edit member records.

> **Too vague:** There is an integrity risk.

Analysed: Because every volunteer shares an administrator account, a volunteer could alter a member's payment status without the change being reliably attributed. This compromises integrity because staff may act on an inaccurate account balance.

Apply the risk-analysis structure

A school canteen app stores allergy details and account balances. At a busy event, staff record purchases on paper and update the app several hours later.

Analyse the scenario to determine one risk to data integrity. Produce one complete risk statement that includes:

- specific evidence from the scenario
- what could happen to the data
- why the consequence is an integrity problem.

View a sample solution

Because purchases are recorded on paper and entered several hours later, a transaction could be missed or entered incorrectly. This compromises integrity because the stored account balances may be inaccurate, so students could be charged the wrong amount.

One incident can have several effects

The triad is a thinking tool, not three sealed boxes. One incident may compromise several properties, but each claim needs its own cause and consequence.

Imagine ransomware that encrypts a medical clinic's patient files and sends a copy to an attacker:

- **Confidentiality:** the attacker possesses private patient data.
- **Integrity:** records may have been altered and can no longer be trusted.
- **Availability:** clinicians cannot access records needed for care.

> **Avoid this trap:** Do not force all three properties into every scenario. Select only those supported by the evidence.

Identify each affected property

A malicious user deletes the only copy of a community centre's booking database after reading the contact details inside it. **Analyse** the incident and identify every CIA property directly compromised. **Justify** each choice with a different consequence.

Check your answer

- **Confidentiality:** an unauthorised user viewed customers' contact details, which exposes private information.
- **Integrity:** deletion is an unauthorised change to the stored data, so the database is no longer complete.
- **Availability:** staff cannot access booking information because the only copy has been deleted.

Privacy and confidentiality are different

> **Privacy** concerns how personal information is collected, used, disclosed and managed, including people's expectations and rights. **Confidentiality** concerns preventing unauthorised access or disclosure.

A confidential dataset can still create a privacy concern. For example, an organisation might securely restrict access to location data but collect far more of it than its service needs. No outsider saw the data, yet the collection may still be inappropriate.

Privacy, confidentiality or both?

For each scenario, identify whether the main issue is confidentiality, privacy, or both.

1. An employee posts a customer's private support message publicly.
2. A fitness app collects precise location every minute even when its route feature is turned off, but keeps the data securely restricted.
3. A clinic collects relevant health data for patient care, but an unauthorised contractor reads it.

Check your answer

1. **Both:** personal information has been disclosed inappropriately and confidentiality has been compromised.
2. **Privacy:** the concern is excessive collection, even though access remains restricted.

3. **Both:** the collection has a legitimate purpose, but unauthorised access compromises confidentiality and the handling of personal information affects privacy.

Independent investigation: the late-night library

A public library launches an after-hours locker service. Members reserve items in an app, then enter a six-digit collection code at a locker terminal. Consider this system:

- The terminal displays the previous member's full name and borrowed titles until the next person enters a code.
- Staff sometimes mistype locker numbers when adding reservations manually.
- All locker terminals rely on one network connection. If it fails, no reserved item can be collected.
- Members need the service after the staffed library has closed.

On paper, **analyse** the scenario to **determine** one risk to each part of the CIA triad. For each risk, write:

1. the relevant scenario evidence
2. the event or data problem that could occur
3. the consequence that **justifies** your classification.

View a sample solution

- **Confidentiality:** Because the terminal continues to display the previous member's name and borrowed titles, the next user can view information they are not authorised to access. This compromises confidentiality and could reveal sensitive reading interests.
- **Integrity:** Because staff manually enter locker numbers, a typing error could link a reservation to the wrong locker. This compromises integrity because the stored reservation would not accurately represent the item's location.
- **Availability:** Because every terminal depends on one network connection, a connection failure would prevent valid codes from being checked. This compromises availability because authorised members could not collect items when staff are unavailable to help.

Revision #5
Created 2026-10-06 00:39:27 UTC by Mr Napper
Updated 2026-10-06 01:31:54 UTC by Mr Napper