What Is Security

```
module = Module(
    code="ELEE1171",
    name="Securing Technologies",
    credits=15,
    module_leader="Seb Blair BEng(H) PGCAP MIET MIHEEM FHEA"
)
```

Download as a PDF

Some Terms to Note

- 2FA – Two-factor Authentication
- ACL – Access control list
- BIA – Business Impact Analysis
- 5G – Fifth generation cellular network telephony
- BCP – Business Continuity Plan
- CC – Common Criteria
- CCTV – Close Circuit Television
- CERT – Computer Emergency Response Team

Content

- What is security
- CIA
- Threats | Risks | Vulnerabilities
- Encryption
- Privacy
- GDPR
- BCP | IRP | CP
- What is management?
- Do I need to be technical for Cybersecurity?

What is Security?

Introduction

Two main objectives of Security:

- Making sure authorised personnel have access to the resources they need
- Making sure unauthorised personnel do not have access to the resources
- Authentication is the procedure of confirming the identity of the user trying to access certain data
- It is a mandatory element of security model

What are we protecting?

Assets: Anything **of value** to your Organisation

- Hardware
- Software
- Staff
- Data
- Network

Lives:

- This is because Cyber Security involves protecting beyond your Organisation. E.g. Citizens of a Country, customers, children etc.

What are we protecting?

Asset types

- Physical Assets: know any?
- Pure information/Data
- Software: for managing or processing information

What are we protecting from?

- **Threats:**
  - Something that can cause harm to assets
- **Vulnerability:**
  - a weakness or loophole that can be exploited by a threat
- **Risk:**
  - Chances that something will happen OR effect of uncertainty. E.g:
    - Walking into a crowd during the pandemic without a face covering increases your chances (or Risk) of catching the virus.
    - Wearing a mask also does not totally eradicate it but mitigates the chances.
- **Impact:**
  - How much it affects our **business** | **operations** | **assets**

Bringing all together;

- A threat needs a vulnerability
- A vulnerability is a loophole that a threat can take advantage of
- A threat would usually need a vulnerability to be successful
- It is risky to your business if you have vulnerabilities that threats can exploit

Main Goals of Security

Confidentiality:

- Only authorised subjects can view or access information. If you are not authorised, no access. If you do not have clearance, no access.

Integrity:

- Information is not modified illegally or by an unauthorised subject. Can also mean a system is working as it is supposed to. E.g. patient monitor at hospitals. {Accuracy and completeness}.

Availability:

- System is available when needed or queried. That is, it responds when it is expected to. Availability can affect both data and system. E.g. Ransomware

Strategic alignment:

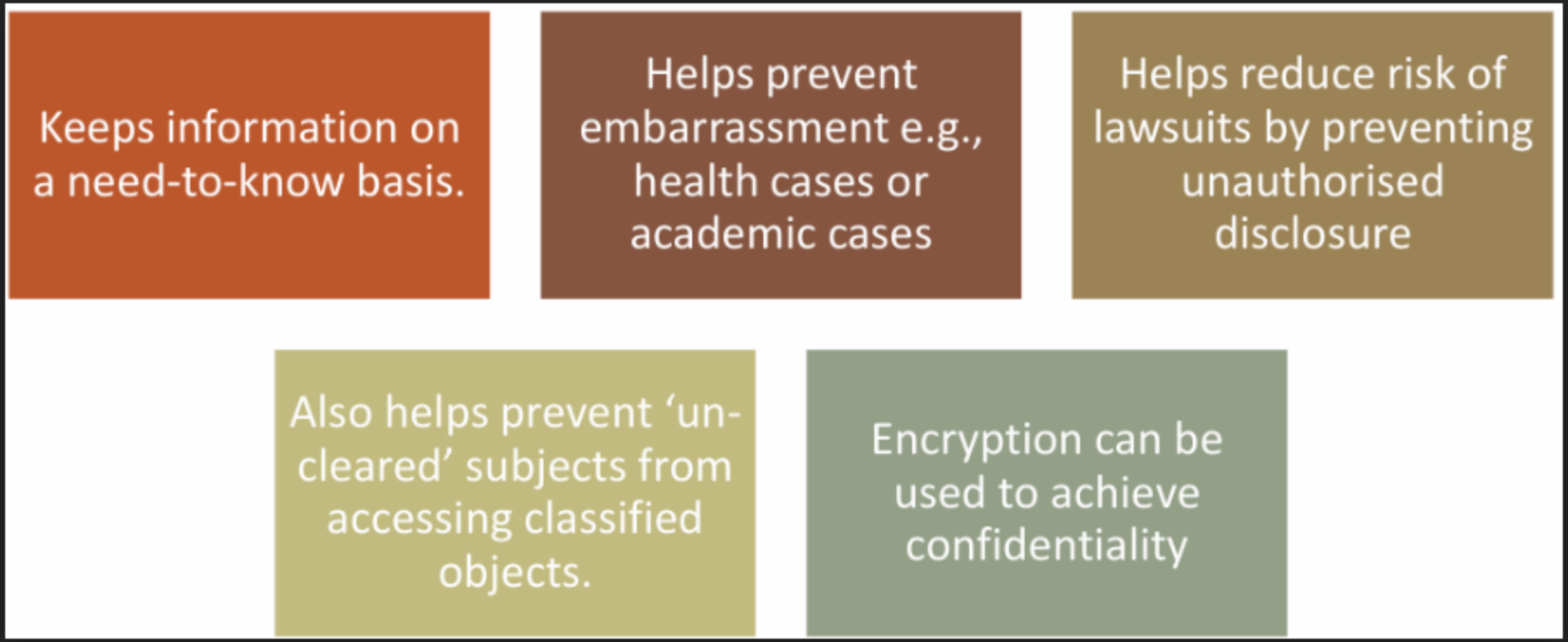
- All the above need to work together towards achieving the Company’s goals

Information Security Principles

DAD Acronym {Opposite of the CIA}

- Disclosure:
  - Unauthorised disclosure of sensitive information can lead to severe privacy breaches and compromise the security of an organisation
- Alteration:
  - Data alteration by malicious actors can corrupt critical information, making it unreliable and potentially harmful.
- Destruction/Denial:
  - Destruction or denial of access to essential data can disrupt operations and cause significant losses for businesses

Why is confidentiality important?



Keeps information on a need-to-know basis.

Helps prevent embarrassment e.g., health cases or academic cases

Helps reduce risk of lawsuits by preventing unauthorised disclosure

Also helps prevent ‘un-cleared’ subjects from accessing classified objects.

Encryption can be used to achieve confidentiality

Subject vs Object

- Subject: makes request to access/use an object

```
curl -S https://path/to/url --data $(cat)
```

- Objects: the resource a subject needs access to

```
{
  "id": 1001,
  "title": "Who invented JSON?",
  "author": {
  "name": "Douglas Crockford"
  },
  "tags": ["api", "json", "programming"],
  "published": false,
  "publishedTimestamp": null
}
```

Importance of Integrity

- Helps ensure information is unchanged between source and destination

```
Your Hash: 2f2bae6733b6449f88b7c372108c1eb7
Your String: "This MD5 generator is useful for encoding passwords,"
```

- Hashing can be used to easily compare files and spot those that have been altered (by comparing their hashes)

```
Your Hash: 441ab12d5386b0eb6755df60bccb5b08
Your String: "This MD5 generator is useful for encoding passwords"
```

Practical- How to check for file Integrity

Windows

```
certutil   -hashfile    <filename>    <md5, sha1, sha256, sha512>    [ENTER]
```

Linux/Mac

```
<md5sum, sha1sum, sha256sum. sha512sum>   <filename>  [ENTER]
```

* The major difference between Hashing and Encryption is that: No keys are used in hashing but only algorithms e.g., MD5

Why is availability important?

- Using an e-commerce site for example
- Customers should always be able to buy. If the site is not reachable, no sales, and if no sales, no profit.Continuous lack of profit = loss of business
- Not being reachable could also affect the business’s reputation and furthermore push customers to competitors.

| *Information that is not available when and as required is not information at all but irrelevant data |

The Security and Operational Triad

CIA Triad (Information Security)

Confidentiality (C): Ensures that sensitive information is only accessible to authorized individuals, preventing unauthorized access or disclosure.

Integrity (I): Maintains the accuracy and trustworthiness of data by preventing unauthorized modifications.

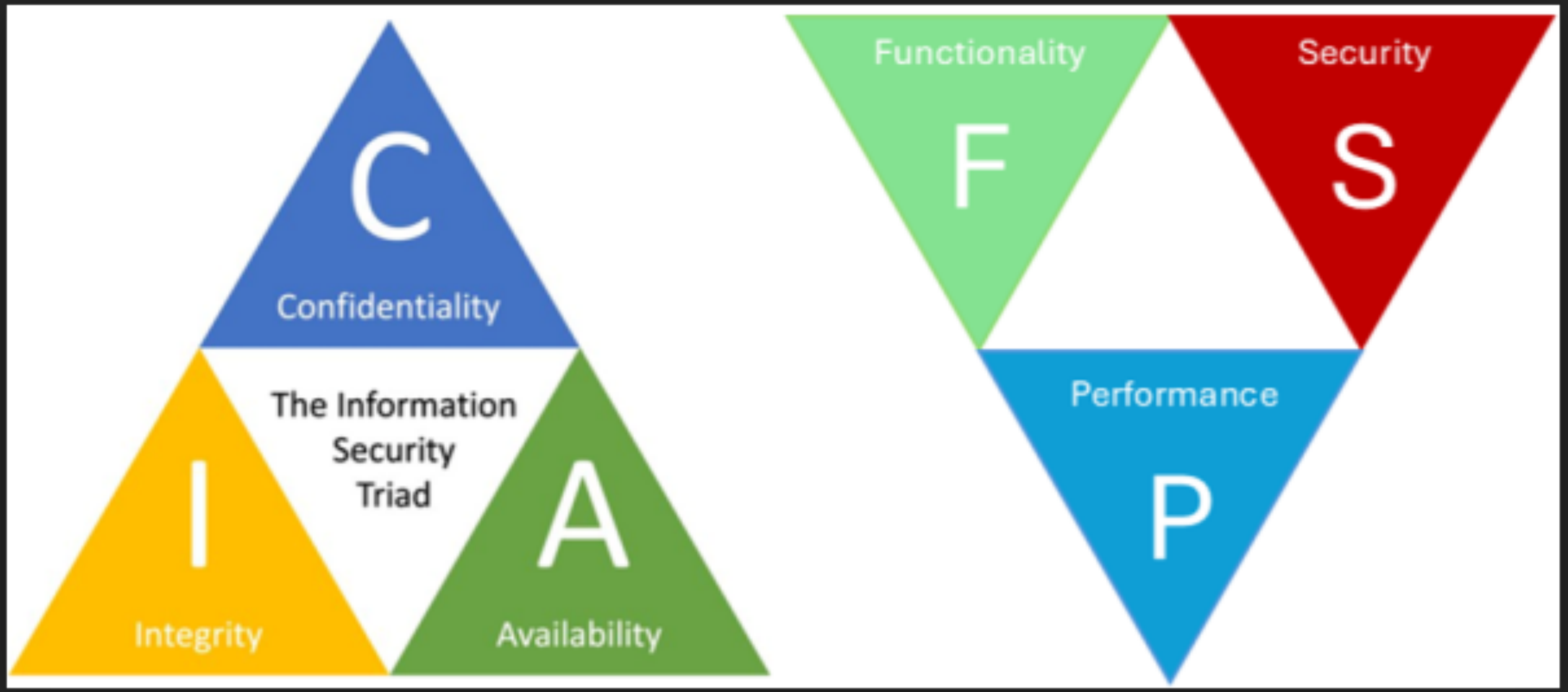
Availability (A): Guarantees that information and systems are accessible to users when needed, ensuring reliable access.

FSP Triangle (Design Trade-offs)

Functionality (F): Refers to the features and capabilities a system provides to meet user and business requirements.

Security (S): Involves protecting systems and data from threats, often requiring compromises with functionality or performance.

Performance (P): Measures how efficiently a system runs, including speed and responsiveness, which can sometimes conflict with security measures.



Information Security Principles

5 Supporting A’s

- **Authentication:** verifying credentials or identity
- **Accountability:** Ability to trace actions back to the source
- **Auditing:** Checking for controls and compliance
- **Assurance:** Confidence that systems are working as intended
- **Accounting:** Property of recording every action taken by subjects on objects (logging)