Concepts that underpin Information Security Management –

1. Confidentiality
2. Integrity
3. Availability

Some also add,

1. Non-repudiation

**Confidentiality:** Information is not made available or disclosed to unauthorized individuals and entities or processes.”  (Campbell, 2016).

**Integrity:** the property of accuracy and completeness of assets.” (Campbell, 2016).

**Availability:** the property of being accessible and usable upon demand by an authorized entity.” (Campbell, 2016).

**Non-repudiation:** ability to prove the occurrence of a claimed event or action and its originating entities.” (Campbell, 2016).

A picture containing text, businesscard, accessory

Description automatically generated

# Availability

The UK government implement three categories to comply with Availability in the triage.

Official 🡪 Secret 🡪 Top Secret

The vast majority of documents will be classified as Official, whereas only assets that could cause major military, commercial or international issues would be classified higher. The same security products and systems may be used to manage all three categories, with enhanced settings or processes employed for the higher security category items. For example, the processes in place may define what assets can be sent via email, who they can be sent to (I.e. within the Government network or outside it) and what controls should be applied.

Availability is probably the 'tenet' that is most dependent on processes. To ensure 'reliable and timely access to data and resources' (Campbell, 2016) there needs to be processes in place to ensure Business Continuity (BC) and Disaster Recovery (DR).

|  |  |
| --- | --- |
| **Recovery Time Objective** | **Recovery Point Objective** |
| Recovery Time Objective (RTO) is concerned with how quickly a service needs to be recovered - I.e. available for use. | Recovery Point Objective (RPO) is concerned with how much data can be lost – which is usually dependent on whether data can be easily retrieved or reconstructed from other sources or whether it is unique to the system in question. For example, running nightly backups can be a perfectly adequate DR solution if the RTO is measured in days, but it would not be suitable for an online system that guarantees less than fifteen minutes of downtime. |

Human element always the weakest point.

Availability is probably the 'tenet' that is most dependent on processes. To ensure 'reliable and timely access to data and resources' (Campbell, 2016) there needs to be processes in place to ensure Business Continuity (BC) and Disaster Recovery (DR).

This is a sub-topic in itself as it will depend on risk assessment, business impact assessments (BIA) and the solution provided will depend on two critical parameters – the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO).

# Integrity

To avoid processes being changed by an unauthorised person or in a unauthroised way.

# **Non-repudiation**

messages need to be signed in a non-disputable manner.

Technology adds real value to this tenet, not only can public key encryption/infrastructure (PKE/ PKI) be used to sign messages in a secure and non-disputable manner, but automation can be used to ensure that all messages sent are signed in this way.

Coordinated Vulnerability Disclosures (CVD).

Diagram

Description automatically generated

## Open Design e.g. not security through obscurity

The third principle – open design – is related to the first in that it recommends that security controls are obvious and well documented, rather than attempting to complicate a system in an attempt to achieve 'security through obscurity'. The reality is the latter rarely works in practice, but it does make attacks and/or attackers much harder to find. The security policy should be separated from the security mechanism.

# Best security standards, principles, and best practice

Despite being published in 1975 – principles introduced by Saltzer and Shroeder in The Protection of Information in Computer Systems" - are still valid today.

## Principles for the Protection of Data

|  |
| --- |
| Economy of Mechanism e.g., simple design The first principle – economy of mechanism – is similar to Antoine de Saint-Exupery's quote about perfection. For example, some people will use multiple back-to-back firewalls, sometimes from different vendors, in order to make a system more secure. This is listed as an anti-pattern by the NCSC (2019) because it increases complexity, maintenance and management overhead for little or no security benefit, as well as making attacks and weaknesses much more difficult to detect. It also breaks the first 'best practice' principle. |

|  |
| --- |
| Least Privilege e.g., sudo or UAC The second principle – least privilege - is well understood and embraced. For example, Microsoft in their latest desktop OSes set the default user to NOT be the administrator. (This has been enshrined in Unix-like operating systems for many years with the "sudo" command giving the user temporary 'root' privileges). |

|  |
| --- |
| Fail-safe Defaults e.g. deny first The fourth principle – fail-safe defaults – basically says "lock everything down". That is, do not run services that are not explicitly required, close ALL unnecessary network ports and create the minimum number of users possible. Only install a service, add a user or open a port if it is explicitly required by the system or application. In addition, if a service or system fails, it should fail safely – which often means closed or not active. |

|  |
| --- |
| Fail-safe Defaults e.g. deny first The fourth principle – fail-safe defaults – basically says "lock everything down". That is, do not run services that are not explicitly required, close ALL unnecessary network ports and create the minimum number of users possible. Only install a service, add a user or open a port if it is explicitly required by the system or application. In addition, if a service or system fails, it should fail safely – which often means closed or not active. |

|  |
| --- |
| Separation of Privilege e.g., 2FA The fifth principle – separation of privilege – is related to principle 2, but it says as well as using the least privilege levels possible, you should also aim to enforce those privileges through multi-factor authentication, such as using a password and an external token. |

|  |
| --- |
| The Least Common Mechanism e.g. avoid shared resources, also known as defence in depth The sixth principle – the least common mechanism – recommends the use of security tiers and partitioning functions between tiers. For example, an application server, database server, and cache should all run in separate zones, ideally on separate virtual machines or even physical ones. |

|  |
| --- |
| Complete Mediation e.g., ACL checks at regular intervals The seventh principle – complete mediation – recommends the use of a service (or daemon) that regularly checks the status of key files for evidence of tampering. Such services are referred to as intrusion detection systems (or IDS). In addition, it must also maintain active lists of authorised users so that if permissions have been revoked, the system is notified and updated immediately. |

|  |
| --- |
| Psychological Acceptability also known as least astonishment The eighth principle – psychological acceptability – is a less obvious principle. It is concerned with the effect that security mechanisms and controls may have on the average user. For example, if utilising a security control is too onerous, users may try to circumvent the controls or stop using the system altogether. A common example is passwords – if the system requires that passwords are too complex, users may try and reduce the cognitive load by writing down passwords. This obviously bypasses the security control, especially if the written passwords are kept in plain sight such as stuck onto system screens and suchlike. |

|  |
| --- |
| Work Factor e.g. longer passwords, 256 bit keys, etc. The ninth principle – work factor – is often related to the eighth principle above. As the authors assert "work factor is concerned with the cost of circumventing a security control" (Saltzer & Schroeder, 1975). A commonly quoted example concerns password complexity – simple 4-character alphanumeric passwords have only 26^4 = 456 976 combinations, which can be cracked by a modern computer in seconds. Thus, more complex passwords are obviously required but there is a trade-off required with psychological acceptability as discussed previously. Modern approaches include the use of passphrases instead of passwords, and using multi-factor authentication, as also discussed previously. There are alternatives to help manage more complex passwords, such as password managers. |

|  |
| --- |
| Compromise Recordings e.g., auditing and logging – includes continuous improvement The tenth and final principle is compromise recordings which is the principle of recording access and changes to a system. This is a well-known and supported approach in modern systems, performed by modern logging and auditing solutions. |

# Kill chain deployment

An often-recommended strategy is to think like an attacker when trying to establish the best defence for a system. Similarly, one of the aspects of the vulnerability assessment process is to try and compromise a client's system. Lockheed Martin is a well-known military and commercial enterprise contractor and they produced (and documented) a 'penetration-testing’ approach known as the Cyber Kill Chain.

A picture containing graphical user interface

Description automatically generated

# Scientific method

# A screenshot of a computer Description automatically generated with low confidence

It was first postulated by Aristotle (Poppi, 2004) as a form of empirical investigation, but it has been reiterated, reused, and in some cases 'rediscovered' by many philosophers throughout the ages. So much so that it is widely applicable to many domains and sub-domains.

1. Firstly the use of observation to raise questions about the subject under investigation.
2. Secondly research to establish ground rules and basic concepts.
3. Thirdly the formulation of a hypothesis to prove (or disprove).
4. Fourthly a test phase where the hypothesis is tested.
5. Fifthly the analysis of the data – is the hypothesis supported or falsified.
6. Sixthly report findings and conclusions and suggest next steps or further work required.