**The Threat and Vulnerability Landscape**

**Security** should be selected specifically against the **threats** percieved from the particular **adversary**

**Security** is a technology, as well as actions and processes

**Assets** are ‘things’ that are necessaqry to be protected

* If they were compromised or lost, bad things would happen

This process is done at the beginning of the whole prosses during the **risk assessment stage**

The **higher** the level of security, the **lower** the ease of use is

* So, it is important to **define specific assets** so that security measures can be tailored and minimised on **how burdensome the security level will be**

Concentrate on **consequences and impact** to determine your assets

**Risk Assessment**

1. Asset
2. Vulnerability
3. Threat
4. Adversary
5. Consequence

**What does “secure” mean to you?**

The way to consider the type of security control we may need for an asset is to think about the asset in terms of its **security attributes**, its needs for **confidentiality**, **integrity** and **availability**

* **Confidentiality**
  + Do we want the asset to be not disclosed
  + If this is true, then we understand we need confidentiality controls
    - Encryption
    - Digital Signature (+ Encryption)
* **Integrity** 
  + Do we want to make sure the asset is not altered, ensure the accuracy and completion of the asset
  + Cannot be modified in unauthorised manner
    - Hash
    - Digital Signature (+ Encryption)
* **Availability**
  + Do we not want it destroyed, the asset must be available and functioning when needed
* **Possession**
  + Loss of possession or control of an asset that doesn’t breach confidentiality
* **Authenticity**
  + Do we need the claim of origin or authorship of the asset to be true
  + Utility/Usefulness, ransomware that encrypts a user’s data can render the asset useless with no utility
    - Digital Signature (+ Encryption)
* **Non**-**repudiation**
  + Ensures that someone fulfils their obligation to a contract
  + The sender can’t deny that they sent one part of the transaction and vice versa
    - Digital Signature (+ Encryption)
* **Authentication** / **Authorisation**
  + Who is allowed access to the asset
  + Verifies the identity of the asset
  + Is it what it claims to be
    - Digital Signature (+ Encryption)

**Asset 🡪 Security Attributes 🡪 Security Controls**

SABSA Security attributes

* Stationx.net/sabsa

**Defence in Depth**

Provide layers of defences so if one fails, another continues to protect

**Three main types of protection**

**Prevention**

* Encrypt files and ensure that keys or passwords aren’t available
* Prevention defence to stop assets being compromised

**Detect**

* Set up a canary, deliberate trap where a hacker or malware will trigger a notification to you

**Recovery**

* Having the ability to recover a lost asset
* What you cannot prevent, you detect
* What you cannot detect, you recover

**Zero Trust Model**

Everything that is done involves a factor of risk. Some acceptable, some not.

* We can mitigate risk by distributing the trust
* Trust nothing, evaluate and distribute the trust

Example

You need to store files on drop box for ease of access and back up

You can’t trust that drop box won’t read, lose or change your files

* You distribute the trust to yourself
  + You back-up the files yourself in a different location
  + You encrypt the files, client-side, using a hash only you have the key for before uploading

You need to download an application that has no security audits

* You run it in an isolated VM to stop any malware getting out