**CIA**

The guiding principles behind information security are summed up in the acronym CIA (and we’re pretty sure there’s a joke in there somewhere), standing for confidentiality, integrity and availability.

We want our information to:

* be read by only the right people (confidentiality)
* only be changed by authorised people or processes (integrity)
* be available to read and use whenever we want (availability).

It is important to be able to distinguish between these three aspects of security. So let’s look at an example.

**Case study: Equifax, credit reporting company**

In September 2017 Equifax reported a data breach in which the records of 147 million people had been exposed, mostly of people in the US, but 693,665 people in the UK also had their data exposed. Equifax UK later wrote letters to each of these people explaining the situation.

The exposed data contained millions of names and dates of birth, Social Security numbers, physical addresses, and other personal information that could lead to identity theft and fraud. Equifax had a system to monitor network traffic, but it wasn’t working for the previous 19 months because a security certificate hadn’t been renewed.

Equifax stored its data in a database called ACIS, and was alerted in March 2017 to a critical security vulnerability in an Apache Struts web server that provided access to this database. A patch had been issued but Equifax failed to ensure that the patch was installed. Hackers exploited this vulnerability until the missing certificate was installed at the end of July 2017.

In May 2019 the data breach was thought to have cost Equifax $1,400,000,000.

In July 2019 Equifax agreed a settlement with The Federal Trade Commission (US) of over $575,000,000 (perhaps up to $700,000,000) with a free monitoring and identity theft service for up to 10 years.

So how do the principles of CIA apply to the Equifax case? Quite obviously, confidentiality was violated: unauthorised people could read the data. However, authorised users still had full access to the data, so it remained available; and the data was not changed, so its integrity was preserved.

**Information assets**

Time for another definition. When talking about valuable data we use the term ‘information assets’. In the Equifax case the information assets were the data about people and their financial records, collected by Equifax.

When we consider security of online communications and services, we also need two additional concepts: ‘authentication’ and ‘non-repudiation’.

When we receive a message, we want to be confident that it really came from the person we think it came from. Similarly, before an online service allows a user to access their data, it is necessary to verify the identity of the user. This is known as authentication.

Non-repudiation is about ensuring that users cannot deny knowledge of sending a message or performing some online activity at some later point in time. For example, in an online banking system the user cannot be allowed to claim that they didn’t send a payment to a recipient after the bank has transferred the funds to the recipient’s account.

**Malware**

Finally, there are a number of terms associated with software that attempts to harm computers in different ways. Collectively these are known as ‘malware’ (a contraction of malicious software).

Depending on what the malware does, different terms are used in relation to it. For example:

* **ransomware** is malware that demands payment in order to refrain from doing some harmful action or to undo the effects of the harmful action
* **spyware** records the activities of the user, such as the passwords they type into the computer, and transmits this information to the person who wrote the malware
* **botnets** are created using malware that allows an attacker to control a group of computers and use them to gather personal information or launch attacks against others, such as for sending spam emails or flooding a website with so many requests for content that the server cannot cope, called a denial-of-service attack.