**Cyber Security**

**What does it do? (600 words)**

Cyber Security is, simply put, one of the most important parts of the modern world. At a basic level, cyber security is preventing unauthorized operations from happening on computer and information systems, and in particular to protect the information and data stored on those systems. Despite seeming so simple, cyber security is one of the most complex and essential parts of the IT industry.

At the heart of cyber and information security is a concept known as the ‘CIA triad’. CIA stands for Confidentiality, Integrity, and Availability. Confidentiality means that only people who are authorized should be able to access data. Integrity means that when someone accesses data, the data should be intact and untampered with. Availability means that if someone is authorized to access data, they should be able to access it without trouble, and when they need it.

Confidentiality is probably the principle that comes to mind first when thinking about cyber security. People that are not authorized to access a system should not be able to do so. Passwords, biometrics, and encryption keys are all ways of ensuring confidentiality.

Integrity is a very important part of information security. When someone accesses data, they need to know that it has not been tampered with, altered, or infected in any way. One way of keeping integrity is with digital signatures, and encryption using public and private encryption keys, so only authorized users would be able to change the data. Many of these methods also apply to confidentiality and availability.

Availability is the last of CIA triad, and also the most practically significant. What is the use of keeping data confidential and maintaining its integrity, if no one can use it? As much as unauthorized users should not have access, legitimate users and devices need to have access to the systems and information which they are authorized to use.

Maintaining the CIA triad is at the core of cyber security. If a device is hacked, it can breach Confidentiality and Integrity. DoS (Denial of Service) attacks (attacks targeted to shut down a device or server) violate the principle of availability. Having servers that are not properly secured can potentially have problems with all three aspects. How to uphold all three aspects of the CIA triad is essentially the main problem of cyber security.

At the core of the issue is authenticating someone’s identity. If verifying a person or device’s identity could be done with 100% accuracy and trust, cyber security would be far simpler. All three parts of the CIA triad would be essentially fixed. As this is not the case, however, people’s identities need to be verified. There are three main ways to authenticate someone’s identity: Something they know, something they are, and something they own (Scott 2020).

Something only the person knows, usually a password, PIN number, or the like, is one of the easiest (and least secure) ways of verifying someone’s identity. Passwords can be leaked, and PIN numbers can be forgotten, but this is still a good way of proving someone’s identity in the absence of any better options.

The next method of authentication is by checking something that only the person is. This usually comes in the form of fingerprint scanners, facial recognition, and similar biometrics including the more exotic tests like iris scans and DNA matching. Also included in this is places only you can go, like your home. This is arguably more secure than a password but has the downside that if your fingerprint is leaked somehow, there is no way to change it.

The last way of authentication is something that only the person has. This includes physical keys (like your house key), your credit card, and things like your phone, which can be used in things like 2-factor authentication. This also includes things like digital keys, which Google has recently used (Newman 2020).

Ideally, systems and devices should use multiple or all these methods of authentication. Bank cards use multiple methods: A physical card (only you own), a PIN number (only you know), and to an extent, they also use a third method: your location. Many banks keep track of the locations your card is used, and may contact you if your location changes unexpectedly. Websites often have the option of multi-factor authentication: a password (only you know), and your phone (only you own). Many phones have the option of turning on biometrics such as fingerprint scans and facial recognition, which are things that only you are. These principles of the CIA triad and Authentication form the basis of most of cyber security.

**What is the likely impact? (300 words)**

**How will this affect you? (300 words)**

**References**

<https://www.wired.com/story/google-free-security-keys-campaigns/>

<https://www.youtube.com/watch?v=hGRii5f_uSc>