Another presentation on Cyber Security? No, a presentation on Information Security!
Clementine Gritti, August 2021.

In this talk, we cover both the notions of Cyber Security and of Information Security, by defining them and presenting their differences.

In fact, the former is all about protecting data that is found in electronic form (e.g. computers, servers, networks, mobile devices) from being compromised or attacked. Cyber Security aims to protect attacks in cyber space such as data, servers and devices, and deals with cyber crimes, cyber frauds and law enforcement. It is handled by professionals who are trained to deal with advanced persistent threats specifically.

On the other side, the latter is concerned with making sure data in any form is kept secure. Information Security aims to protect data from any form of threat regardless of being analogue or digital, and deals with unauthorised access, disclosure modification and disruption. It is handled by professionals who are trained to prioritise resources first before eradicating the threats or attacks.

Are Cyber Security and Information Security so different? In essence, yes. Cyber Security's goal is to protect against unauthorized electronic access to the data, while Information Security lays the foundation of security of data. In particular, Information Security's main objective is to achieve data *confidentiality*, *integrity* and *availability*. Those three properties are commonly grouped into the CIA triad.

Ransomwares have been very popular and hit the entire world. The term "ransomware" is a combination of the words "ransom" and "software". For instance, a malicious software is spread accross a network with the aim to infect a computer by encrypting the files stored there. Hence, those files become *unavailable*. In exchange of a ransom, the attacker promises the computer's owner to decrypt the files. Since victims put a lot of value onto their data, they are willing to pay the ransom.

Cryptopia was a company from Christchurch offering a platform where customers exchanged various cryptocurrencies (e.g. Bitcoin, Ethereum). A customer could have multiple digital wallets for the different cryptocurrencies he/she owns. However, the start up suffered from a hack, resulting into big losses. In particular, the customers could not access their wallets anymore, hence their cryptocurrencies were no longer *available*. The company was then put into lockdown by the police. Moreover, another hack happened while still into liquidation! There were concerns with the management around the security of the private keys for customers' wallets. The private key is the secret that the owner of a wallet needs in order to trade.

Using new technologies enables to improve farming experience. A regulation has been developed in US about cyber threats in smart farming. The term "smart" stands for technologies emerged from the Internet of Things. However, this means that more data come on stage: more data are collected, more data are shared, more data are processed. Hence more risks of unfortunate data leakage and alteration are likely to happen, threatening data *confidentiality* and *integrity*. By using more devices (e.g. drones and sensors), more risks of disruption are likely to happen, threatening data *availability*.

Implementing Information Security in an organisation can protect the technology and information assets it uses by preventing, detecting and responding to threats, both internal and external. Indeed, most businesses and individuals have information that needs protection. Moreover, threats are everywhere and attacks are getting more impressive, while security breaches are expensive: data breaches cost an average of $3.86 million in 2020 according to Ponemon Institute. Finally, Information Security is simply required by law (e.g. USA Federal Information Security Management Act, EU General Data Protection Regulation).