Cybersecurity

Cybersecurity is comprised of protecting systems, networks, programs and data from cyber-attacks. Usually the attacks aimed to protect users or organisation’s network from unauthorised accessing, changing or destroying information or even damage to the hard drives or power outages from cyberthieves. Currently cyber security is continuing to grow over the years, with its growth in AI machine (Artificial intelligence), digital currencies. As each attack evolve every day as attackers become more creative causing users and organization to increase their network security using common technology such as firewalls, DNS filtering, malware protection, antivirus software and email security solutions. As it is very important to do so, as these attacks can result from stealing identity theft, to extortion attempts and losing important data (E.G: An organisation security breached resulting in their customers detail stolen). Another big notice is to always keep all application or software up-to-date with its latest version to maximize the strong level of security and creating strong and different password for your sensitive accounts.

As for the upcoming future of cybersecurity, many users and organisations would want to develop and adopt technologies as more cyberthreats are growing in both volume and complexity. Where it is a race to secure the systems and devices before they begin to attack and figure out how to manipulate and breach them. One of the most important thing to protect is massive amount of data which is produced by a rapidly growing amount number of devices, meaning more devices means more data. But while data certainly represents a valuable target for fraudsters, it can also benefit the security professionals fight against these cyberthreats. In the cyber world, the attacker activity always leaves a digital trail. This gives security analysts to use this data to predict the attacks and identify malicious actors before striking again. However analysing millions of records can take days and days to trace. It has also shown that “cognitive security” (AI machine) comes in. With its ability to adept machine learning, IT professionals can process the threat data more efficiently, and more accurately predict cyber attackers’ activity. This can be one way of how cognitive computing will outline the future of cybersecurity.

As cybersecurity continue rapidly growing throughout the world and future, many threat comes everyday but each day technologies are being developed and analysed which make a change in the motivation of attackers. Making it possible for the cyber network, gradually increasing its security by adding AI (artificial intelligence), quantum computing, digital currencies and blockchain. As it will be easier than ever to do business and live our lives over the upcoming decade. However, the downside of doing this, is where cybercriminals can use these or modify or even create newer technology to crack and spread new and unexpected threats. Another possibility development that made cybersecurity strong is by developing new and further improving software program such as Antivirus, firewalls and malware protection, adding multiple layers of security allowing users and organisation to minimize the amount of potential threats.

The biggest type of impact of cybersecurity is having it breached, resulting in different type of attacks:

Attack on **confidentiality**: This is most likely stealing, or copying, a targets’ personal information is how many cyber attacks would likely do and start from, even to stealing credit card details, identify thefts or stealing bitcoin wallets.

Attack on **integrity:** As this type of attack is where the cyber criminal would want to sabotage, corrupt, damage and even destroy information or systems, and the people who rely on them, also known as “Phishing”.

Attack on **availability:** This attack is where the cyber attacker would want to prevent the user/organisation from accessing their own data, which is also one of the most frequent type of attack nowadays in the form of “ransomware” and denial-of-service attacks (DDoS). Ransomware encrypts a target’s data and demands a ransom to decrypt. While a DDoS tends to flood a network resource with requests, making it unavailable and overload.

At this moment, cybersecurity continues to grow everyday and what is there for cybersecurity to change, as more and more cybercriminals attacking, it will only be wake-up call to increase the current strength of its security, making it harder for cybercriminal to access. Cybersecurity will usually affect people running a business or organisation because the attacker would want to steal personal information and credit cards or damage the organisation in the form of “ransomware”, leading to the organisation costing millions to repair. It can also affect normal day-to-day user that have access to internet or computer or any smart technology that got internet connection, because attackers can plan a program to even a website you visit and it can randomly download a trojan house program without you noticing it, leading to personal information stolen, data and identify theft and other type of unauthorised access. And yes, I would say it will create and replace redundant with jobs as an organisation can implement an AI (Artificial intelligence) machine that can be faster and trace these attackers.

Cybersecurity will affect my daily life as nowadays everything is mostly on the internet and because of this, I would need to be careful whilst surfing through the web or even checking my email. Where at any time even if I surf the same website on a daily base, where one day a pop up might appear telling me to input my username and password however it usually doesn’t ask you for it because you can only sign in by clicking to the login page. Another could be an instant downloaded program that even the website creator has no idea that this is happening where I would need to be caution at all time surfing the web because I wouldn’t want my computer and personal information, or data taken from me or anyone else. The only different this can make is that if I haven’t got any antivirus and malware protection ill likely have an attack on my computer since I always jump on daily whereas If I installed some antivirus protection, I would need to check my software program to see if its up-to-date and do a daily/weekly scan on my computer to see if there is any suspicious malware installed or downloaded on my computer.

This will usually affect everyone that is using the internet and computer where maybe one of my friend is infected with a virus or malware and it might later spread a chain reaction, leading to his family or people on his internet network to also be infected with the virus or malware.