Cyber Security

By Kirsten Hamilton

Cybersecurity is hard to define accurately, as it encompasses so many levels of IT and is a part of all IT sectors and technologies. Cybersecurity can be defined as the protection of data and systems from unauthorised use or access. The state of cyber security is constantly changing and often new security technologies spawn new technology trends across the board. It is arguably the most integral sector of IT.

Blockchain is an excellent example of how security influences new technologies and shapes how the world develops. The advent of cryptocurrencies using blockchain algorithms to make them decentralised and more secure has bled over into many other sectors and will possibly change the way we use and distribute data, and even has the potential to change our entire economy (Blockgeeks, 2019). If blockchain is used our entire current data structure and network structure would need to change dramatically (Blockgeeks, 2019).

People are the leading resource in cyber security. Teams of security specialists and penetration testers analyse and test systems for companies to shore up defences. There is no single solution for security. Every network and program have potential vulnerabilities, and just as people are the threat to security people are also the solution. Hackers are always finding ways around current security technologies and protocols. Cybersecurity is a constant game of cat and mouse, ‘Pen testers’ trying to find and fix weaknesses before ‘hackers’ find these exploits.

Using software solutions such as encryption, or programs like Kaspersky or Norton are some consumer solutions for cybersecurity (Federal Trade Commission United States, 2017). They update themselves regularly to keep up with the latest attacks and viruses. There are also safety apps like Knox that set up a secure space for sensitive data and to save backups (Federal Trade Commission United States, 2017). These apps create a heavily secured area which can be complicated to access, so it is protected better but is not as convenient for constant access hence its separation from the standard operating system. Much of security is a balancing act between ease of use and access vs safety and security. Additionally, Computer and smart phones Operating Systems and programs also update regularly to fix ‘bugs’, errors or vulnerabilities that could exploited or discovered. Commercially, technologies such as firewalls and internal networks are used to help ensure data security. With the advent and convenience of cloud computing, the practice of internal networks is becoming a rare and expensive process.

It is possible to have systems that are near impossible to hack or access unauthorised, but those systems are challenging to use, unwieldy to navigate and expensive to implement and maintain. The general consumer would not accept this, and so we are always on the edge of being secure and being a breach. It is not so much a case of if you are compromised more a case of how badly you will be compromised.

One hardware security technology that has become prevalent in the last few years is biometrics. Smart phones, laptops, houses and even airports can use biometrics in place of traditional security measures. Biometrics have become a lot more reliable and has many applications beyond identification and access management. Many governments are starting to require biometric data for immigration (Australian Government Department of Home Affairs, 2019). As biometrics develops and becomes more widely in use globally the applications for use are both far-reaching and slightly concerning. At this time, it is difficult to break into biometrics, however, given the advances that happen to break unbreakable security, when it does happen how would the user be able to recover from the breach. One cannot change their biometrics.

The likely impact of the changing nature of Cybersecurity is hard to predict, and one single incident could change the entire face of security and the internet. It is very likely that security features will continue to impact our everyday lives. We have already seen this change over the last 20 year and indeed even the last five.

Cloud computing has changed how we need to secure our data and most of the large-scale breaches we hear about today. Businesses and corporations are using cloud-based Virtual networks for business and operations, and nearly every app now comes with free cloud storage space. The security of cloud-based computing is most likely going to be the focus of Cybersecurity over the next few years if not a leading sector of Cybersecurity itself (Intrinsec,2017.).

Biometrics are used for security on every level in smart phones, and everything from passwords to credit card details can be used with the touch of a fingerprint or scan of an eye. The convenience of biometric security measures will most likely make them a significant part of everyday life. For many of us, they already are used very often; many people have fingerprint locks on their phone and Google/Apple pay Apps (Dealspotr, 2018.). In the future it is likely that many interactions will require biometric imprints, everything users own could rely on biometrics locks for security and activation, much of this technology is already in use it is just not widely disseminated yet.

The effect of the dissemination of biometrics would affect people's daily life in many ways. Again, evidence of this is already apparent. Many people do not carry wallets because their phone or smartwatch can perform the functions of the physical cards and cash contained with it accesses with the touch of a finger. This trend could extend to identity keys and eventually even the phone itself. Conversely, I refrain from storing personal data in cloud-based services. I do not store any sensitive data on my devices or against my biometrics. I do not use Google Pay, and I do not have Apple devices. With how widespread these Technologies are and the fact they are becoming a part of everyday life, much like social media has done, the effect for me personally will be the same as social media, I do not particularly want it, but society does it that way, so I have to use it.

# Works Cited

Australian Government Department of Home Affairs, 2019. *Meeting our requirements.* [Online]   
Available at: <https://immi.homeaffairs.gov.au/help-support/meeting-our-requirements/biometrics> [Accessed 3 April 2019].

Blockgeeks, 2019. *What is Blockchain Technology.* [Online]   
Available at: <https://blockgeeks.com/guides/what-is-blockchain-technology/> [Accessed 3 April 2019].

Federal Trade Commision United States,2017. *Computer security [online]*

Availiable at: <https://www.consumer.ftc.gov/articles/0009-computer-security>

[Accessed 4 April 2019].

S,*Thikkavarapu* : Intrinsec,2017. *Future of cloud computing and cloud security [online]*

Available at: <https://intrinsecsecurity.com/future-of-cloud-computing-security/>

[Accessed 4 April 2019]

M,Quoc: Dealspotr, 2018. *Mobile Payments Survey: Apple Pay Leads Google Pay in Usage and Interest Among Millennials & GenZ in 2018 [online]*

Available at: <https://dealspotr.com/article/mobile-payments-survey-apple-pay-google-pay-millennials-generation-z>

[accessed 5 April 2019]