Cybersecurity is the process of protecting computer systems, networks, devices and programs from all sorts of cyber-attacks (Tunggal 2022). Recently the Australian media has made cyber security the center of everyone’s attention. With recent cyber-attacks on Optus and Medibank private it has exposed the increasingly sophisticated and always evolving danger to hackers accessing and exposing our data. Attackers are always evolving new methods that are generally powered by social engineering and artificial intelligence compared to the once seen traditional data breach we were used to. As our world becomes increasingly reliant on technology as a regular part of life so do we see the development of new security programs such as cloud security solutions, multi-factor authentication and unauthorized access protocols to stay ahead of malware (Tunggal 2022). Risk of cyber-attacks is forever increasing with our ever-growing global connectivity and use of cloud storage devices. As the development of this technology is becoming complicated, as are the cyber thieves with the creation of new malware and cyber threats.

It is now common for most workplace to include cyber security training as part of a new employee’s introduction period. [Staff](https://www.upguard.com/blog/is-cybersecurity-hard) need to be educated about common [cyber threats](https://www.upguard.com/blog/cyber-threat) like social engineering scams, phishing, [ransomware](https://www.upguard.com/blog/ransomware) and other [malware](https://www.upguard.com/blog/malware) programs designed to steal intellectual property and personal data (Tunggal 2022). Cybersecurity can be broken down into four main areas of concentration. These areas are deterrence, detection, prevention and response. Deterrence can use both physical and online strategies to minimize the risk of security breach (Openpath 2022). Deterrence can start as simple as a fence, video surveillance, access gates and authorized only entries to a build. Online deterrence takes the form of passwords, multi factor authorization and captcha technology. Detection may come in the form of physical door alarms, inappropriate computer behavior or uncommon network log in locations. Prevention is seen as a way of slowing down breaches or intrusion. Online this can take the form of multiple layers of access control, data encryption, multi-factor authentication (Openpath 2022). Security breach have become a common part of the cyber world. An appropriate response to this situation is a crucial part of cyber security. Security technology products including building lockdowns, remote access and controls, and the ability to send live video feeds to first responders are all great examples of this component (Openpath 2022).

Covid 19 defiantly changed the world we live in. Before 2020 work from home was unheard of and work remotely was seen as a dream job. Since the global pandemic gripped the world, it is estimate that over 35 million American now work from home or remotely (WEF 2020). This means the number of networks and devices that link home computing to corporate platforms has grown dramatically. HP reports that global cyber-attacks are on the rise by 238% since the biggening of the pandemic (WEF 2020). Companies are having to manage these risks by increased security via virtual private networks, continuous password updates, multi factor authorization and increased cybersecurity/ IT employment. As cybercriminals are consistently developing new schemes and programs, organizations are having to invest and develop in new innovated technologies to try to stay ahead of the crime. Real-time data monitoring is a way companies are continuously updating systems and data that is used to protect the organization from cyber criminals (WEF 2020).

Security professionals can then act on data breaches quickly and avoid the risk of loss. With this data collection organizations can track information over long periods which helps to identify and predict behaviors and anomalies that occur. This method is known as trend monitoring (WEF 2020). New and developing technologies such as Artificial Intelligence and Quantum computing are starting to be used by attackers. There is growing evidence that AI could start being used as defensive tools against attacks (WEF 2020). AI could be the future of cybersecurity, however will this put millions of cyber security experts out of work? Quantum computing has been a powerful way to solve some classical mathematical problems in the past(WEF 2020). If used correctly could quantum computing be used to stay steps ahead of the programs created by cyber criminals.

In 2021 the global cyber security market was valued at approximately USD 139 billion dollars (Fortune business insights 2022). Moving forward the market is only expected to grow exponentially. Estimates are expecting the industry to double over the next 10 years to an value of USD 375 billion dollars (Fortune business insights 2022). Over the last two years the cybersecurity industry as seen dramatic increase in job availability. With the ever-growing demand for security solutions, position in the cyber security industry have risen by 7.7% since the beginning of the global pandemic (Fortune business insights 2022). There is already a growing global shortage of cybersecurity specialists. The ever-increasing need for technology to be in our daily lives and make everything we do easier has driven companies to take up a larger online presence. The negative effects of this have been the increase of criminal active in regard to fraud, theft and data breaches. Moving forward companies of all sizes will be investing more time and money into safely securing their online assets. This will only add to the position and jobs available in the cyber security industry. With opportunities becoming increasing available a recent report from ISACA’s State of Cybersecurity found that 60% of companies were now reporting difficulties retaining cybersecurity professionals (Comptia 2022).

According to the Australian Bureau of Statistics, 2.1 million Australians or approximately 11 percent of the population have experienced at least one type of personal fraud in the last 2 years. That is 1 in 9 Australians (abs 2022). How will it affect you? Most likely someone in your direct family has been affected by fraud recently. Today almost everyone in our society is connected to the internet either by our smartphones, laptops, game systems or smart watches. Whether we are making purchases via online shopping, completing internet banking via an app or simply just storing bank account details, we are all vulnerable to cyberthreats. Cybersecurity is becoming even more important to everyone’s daily life as it protects data from theft and damage. All our devices have multitudes of sensitive information including personal identifiable information, protected health information, intellectual property, data, and government information (Tunggal 2022). Without an antivirus protection service in place our devices cannot defend themselves against malware and cybercriminals. Cyberattacks are attempts to access our devices information that can lead to a loss of money and personal information (Readgov 2022). In our society today Wi-Fi is everywhere and during our daily life we may connect to unprotected free Wi-Fi services multi times a day. Unfortunately, it is a common occurrence to have our financial information stolen and our credit card compromised by fraudulent activities. These days cyber criminals are no longer just targeting large companies but more constantly targeting individuals with ransomware that seeks personal and financial information. They may take smaller amounts of money from credit cards and bank accounts (Readgov 2022).

Cybersecurity more than ever needs to become everyone’s personal responsibility no different to locking your car while inside the shops or home while your away on holiday. The recent increase of data breaches mean that cybersecurity is no longer just important for big business and regulated industries, but now more than ever small business and private citizens are at risk of suffering irrecoverable reputational damage following data breaches (Upguard 2022).

References:

openpath(2022) Security Technology. Available at: https://www.openpath.com/blog-post/security-technology. (accessed 4 January 2023)

World Economic Forum (2020) Available at: <https://jp.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk/> (Accessed 5 January 2023)

Fortune business insights(2022) Cyber Security Market Size. Available at: <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165>

(accessed on 31 December 2022)

Comptia(2022) Cybersecurity trends research. Available at: <https://www.comptia.org/content/research/cybersecurity-trends-research> (accessed: 31 December 2022)

(Comptia 2022)

abs(2022) 1 in 9 Australians experienced personal fraud 2020-21. Available at: <https://www.abs.gov.au/media-centre/media-releases/1-9-australians-experienced-personal-fraud-2020-21> (accessed: 4 January 2023)

Tunggal (2022) Why is Cybersecurity Important? Available at: https://www,upguard.com/blog/cybersecurity -important (Accessed: 3 January 2023)

Readgov (2022) Cybersecurity. Available at <https://www.ready.gov/cybersecurity> (Accessed: 2 January 2023)

Upguard (2022) Cyber Security Important. Available at <https://www.upguard.com/blog/cybersecurity-important> (accessed: 31 December 2022

(Upguard 2022)