1.Cybersecurity

According to the oxford dictionary cybersecurity is:

*“The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.”* (Lexico Dictionaries | English, 2019)

From this definition it is simple to see that cybersecurity is a large umbrella term that describes any measure taken to counter a cyber-attack.

There are many different forms of cyber-attacks that a system can come under. From Denial-of-Services (DoS) attacks to Phishing and eavesdropping attacks there are multiple ways that an unauthorized person may conduct offensive actions against your data/systems.

The act of effective cybersecurity can be broken up into different actions taken at different levels in order to mitigate the risks that the ever-evolving information technology world creates. The first act of cyber security begins at layer one starting with the user, a company will usually implement policies that direct personal to maintain certain standards in order to foster a strong cyber security culture. Some of the basic requirements may involve locking terminals when not in use, not writing down/sharing passwords, and not opening attachments on emails sent from unknown addresses.

Securing entry points to allow only authorised personal entry, restricting access to the server room, and installation of security cameras are some more common practices used to secure data within an organisation.

Another portion of effective cyber security is the software installed on devices, from anti-virus applications to strict firewall settings to the implementation of group policies that only allow approved devices to be plugged into terminals.

Cyber security is quickly becoming a very large part of the information technology world and will continue to evolve as more developments are made throughout the years. Due to the fact that cyber security is not so much a technology as it is a policy there is no way of defining what the “state of the art” of this is, the best form of cyber security would be an air gapped system with tightly controlled access to the hardware that makes the system up. Over the next few years both governments and individual’s capability to conduct offensive cyberwarfare will increase, and to counter this more and more emphasis will be placed on privacy of users and security of systems. As IoT becomes a larger part of our life over the next few years the security and privacy expectations placed on companies will rise.

In April of 2011 Sony’s PlayStation network (PSN) came under a cyber-attack where it is possible that approximately 24.6 million accounts were stolen, and 10,700 direct debit details were stolen (Sony Global - Sony Global Headquarters, 2019). This attack at an estimated cost of $171 million dollars (Cbsnews.com, 2019) is just one example of the impact that a cyber-attack can have, it shows that the implementation of cyber security policies is paramount to the effective and profitable running of an organisation. Over the next few years a larger weight will be put on cyber security this has already been trending as you can seen by the average salary of a security expert sitting at number 12 on the top 20 highest paying jobs in Australia (Seek Market Insights AU, 2019) this shows that employers are seeking cyber security experts and understand they are valuable so they are willing to pay more for them.

Further development of cyber security is a necessity as more and more advanced methods of conducting cyber-attacks are becoming prevalent in society today. This technology will continue to grow at an exponential rate. Cyber Security will affect everyone that uses any form of IT equipment. This is why I feel this technology will continue to grow and expand.

I believe that due to the current direction cyber security is moving in it will eventually affect everyone that uses information technology. However, it will affect me in two main different aspects of my life. Firstly, in a personal aspect I already utilise some cyber security techniques such as securing my local network at home by ensuring I use strong passwords for both my router configuration and network access, hiding my SSID and ensuring my home router has the most up to date software, Not opening emails from unknown senders and ensuring I have up to date antivirus software are just some small examples of cyber security practices I use in my personal life. The next aspect of my life cyber security will affect me is in a professional property, I currently work in a sector that focuses heavily on telecommunications systems for a large organisation. Due to the development of cyber capabilities my employer has begun training and employing cyber security experts in order to better protect ourselves from individuals or organisations with malicious intent. Due to this my workplace has also begun to implement more stringent security policies and have begun conducting internal testing of these policies. My workplace has also begun implementing mandatory cyber security training each year that requires each employee to complete a test to pass. In terms of my family and friends cyber security will affect the majority of them in a similar way to me, however for the elderly who do not have as much knowledge in relation to this topic and information technology they may be affected more adversely as they would be seen as easy targets with less safe practices being put in place. This could be mitigated though by further education of the general public and by providing tailored assistance to the elderly.