Most people not involved in the Information Technology Sector who hear the word Cybersecurity think of anti-virus programs for their personal computer. Truth be told Cybersecurity encompasses so much more. Digital Guardian (2020) describes Cyber security as;

*The body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.*

To put it simply Cybersecurity protects infrastructure and information in a world where Cyber Attacks are more and more common. The scale of Cyber Attacks is staggering with 7.9 billion records having been exposed by data breaches in the first nine months of 2019. (Risk Based Security 2019)

Like physical security on a house or business such as a lock or security screen, Cybersecurity protects your personal data and digital devices. Importantly Cybersecurity isn’t simply powerful anti-virus programs, but also training and risk management with an emphasis on evolving with the technology as it becomes more sophisticated and advanced.

Cybersecurity can be broken down into numerous equally important fields which include but are not limited to;

* Network security
* Applications security
* Information security
* Operational security
* Data Security
* Identity management
* Database and Infrastructure security
* Disaster recovery & business continuity
* End-user education

The primary reasons to have adequate Cybersecurity are Cyber Crime and Cyber Terrorism.

Cyber Crime includes everything from identify theft; the use of fake emails to get personal information (Phishing), shutting down or misusing websites, distribution of child pornography. Medical devices have also been targets such as cardiac implants.

Cyber Terrorism includes a cyber-attack on critical infrastructure including dams and power stations.

As hackers become more sophisticated, so too will Cybersecurity technology as continued improvement and innovation race to keep our data secure. Currently only government institutions in Australia and some larger businesses employ Cybersecurity experts to monitor their systems complete upgrades and actively monitor and defend their networks. You might ask as a smaller business, who can’t afford to employ a Cybersecurity team, “what can be done now to protect against these threats?” The answer is simple, better education, up to date anti-virus software and the use of a Web Application Firewalls. These simple steps will help you be more secure in modern times while new technology is still being developed.

There are several areas in which Cybersecurity is being developed and improved that are classed as state of the art technology that will be very important in the future:

**Big Data**

Big Data is an upcoming technology which some say will have a big impact on the Cybersecurity Space. Big Data will allow analysts to examine large and diversified amounts of system data instantly and in real time. This means that irregularities such as cyber criminals intruding into a system can be detected and stopped quickly, to prevent the theft of data or damage being done to critical systems. Although Big Data is still in its early stages, the results of its use so far in the Cybersecurity Sphere appear to be extremely promising. As the technology continues to be refined some are calling Big Data the new Guardian Angel of Cybersecurity.

**Artificial Intelligence and Machine Learning**

Another area progressing quickly in the Cybersecurity space is Artificial Intelligence coupled with Machine learning. This new upcoming technology will greatly improve security against cyber threats by being smarter and faster than humans. Examples of current technology utilising Artificial Intelligence in Cybersecurity are Biometric logins for computers, company systems and smart devices such as phones and tablets. Perhaps the biggest benefit of AI and Machine Learning is that hackers and some organisations sponsored by foreign governments are themselves using AI to infiltrate, corrupt and steal data more frequently. By continuing our own improvements of AI and Machine Learning we can fight AI with AI. Balbix.com says that AI will be able to instantly spot any malware on a network, guide incident response and detect intrusions before they start”.

These state-of-the-art processes are made possible with advancement in hardware, software and the big leaps forward experienced by the Machine Learning and Artificial Intelligence sectors.

**What is the likely impact?**

As technology in Cybersecurity continues to improve to fight cyber crime and terrorism, the development will drive the percentage of cyber crime attacks down. People most affected by the future development of Cybersecurity Systems will be criminals and foreign governments who currently engage in wide spread cyber terrorism such as China. China currently utilises cyber-attacks to steal technological secrets. The impact can be seen clearly with a recent attack on Australian organisations across a range of sectors such as government, industry, education and health in 2020. The positive side of development and new future technologies in Cybersecurity will be the company data, technological secrets, health and financial data will be safe from theft. This will especially benefit the elderly in our communities who most unfortunately are not very tech savvy and are regularly the victims of cyber-crime.

The progressions of technology in the Cyber Security’s space will continue to make jobs. As smaller businesses become more aware of the threats of Cybercrime, upgrades to security systems will increase creating jobs. Jobs will also increase in the education section of Cybersecurity as more companies realise that they need to educate employees of the dangers to make the work environment a safe place.

Not only is the demand for Cybersecurity professionals high in Australia, but it is high across the world. Michael Brown CEO of Symantec (2016) said “There are currently one million cyber security jobs globally. This demand is projected to increase to 6 million by 2019, with an expected short fall of 1.5 million”.

**How will this affect you?**

In my opinion cyber security will have a big impact on my life going into the future. As Cybersecurity capabilities grow, so will the abilities of people who wish to steal data and attack infrastructure across the world. I believe it is only a matter of time before a large-scale attack directly affects me, be it though my credit card data being stolen or something more serious, such as the power to my house or business being affected by an attack on the nation’s power grid. What will be different for me in the future is I will now work harder to be better prepared and aware of Cybersecurity.

I will ensure my family and friends know about the need for Cybersecurity to protect themselves. I will help them understand the need for regular software updates on their personal devices to help keep them safe. I will help educate family members about the seriousness of Cybercrime and need for Cybersecurity. In particular I will ensure family and friends know to keep an eye out for the following threats;

* Suspicious Links
* Password promiscuity
* Mal Ware
* Phishing emails

I hope by educating myself and my family and friends we can all understand how to protect ourselves adequately utilising Cybersecurity.

I am interested to see in the future how technology will grow and and change for the better to provide better protection for my personal details and data.

**References**

De Groot, J 2020, *Cyber Security*, Digital Guardian, viewed 12 July 2020, [https://digitalguardian.com/blog/what-cyber security#:~:text=Cyber%20security% 20refers%20to%20the,to%20as%20information%20technology%20security.](https://digitalguardian.com/blog/what-cyber%20security#:~:text=Cyber%20security% 20refers%20to%20the,to%20as%20information%20technology%20security.)

Kaspersky 2020, *What is Cybersecurity*, viewed 9 July 2020, <<https://www.kaspersky.com.au/resource-center/definitions/what-is-cyber-security>>.

CISCO, *What is Cybersecurity*, viewed 9 July 2020, <[https://www.cisco.com/c/en\_au/ products/security/what-is-cybersecurity.html#~how-cybersecurity-works](https://www.cisco.com/c/en_au/%20products/security/what-is-cybersecurity.html#~how-cybersecurity-works)>.

Forbes 2016, *Cybersecurity Jobs*, viewed 14 July 2020,<

[https://www.forbes.com/sites/](https://www.forbes.com/sites/ stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#647f8c1f27ea)

[stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#647f8c1f27ea](https://www.forbes.com/sites/ stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#647f8c1f27ea)>.

Cyber Threat Portal 2019, *Elements of Cybersecurity*, viewed 13 July 2020,

<<https://cyberthreatportal.com/elements-of-cybersecurity/>>.

Disruptor Daily 2019, *Future of Cybersecurity*, viewed 15 July 2020, <<https://www.disruptordaily.com/future-of-cybersecurity/>>.

Risk Based Security 2019, *Number of Records*, viewed 14 July 2020, <<https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/>>.

Baranchuk, Adrian, Refaat, Marwan M, Patton, Kristen K, Chung, Mina K, Krishnan, Kousik, Kutyifa, Valentina, Upadhyay, Gaurav, Fisher, John D, and Lakkireddy, Dhanunjaya R. "Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know?" *Journal of the American College of Cardiology* 71.11 (2018): 1284. Web.

Everett, Cath. "Big Data – the Future of Cyber-security or Its Latest Threat?" *Computer Fraud & Security* 2015.9 (2015): 14-17. Web.

Norton 2020, *Emerging Threats Personal Impact Cyber Crime*, viewed 15 July 2020, <<https://us.norton.com/internetsecurity-emerging-threats-personal-impact-cybercrime.html>>.

Balbix 2020, *Insights Artificial Intelligence in Cybersecurity*, viewed 14 July 2020, <http://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/>.