**Cybersecurity**

**What does it do?**

As stated by (Kaspersky, n.d) Cybersecurity is the implementations to defend computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It has numerous categories and in practice is the security systems in place that protects any electronic device. Technology is growing in all forms and is a key to future development but with this brings new security challenges. With new programs and technology being introduced at an exponential rate the ways in which can be compromised is also continuing.

**What can be done now?**

In its current state we have access to numerous safeguards such as Data Loss Prevention, IDS, IPS, SIEM, Firewalls and Antivirus. Many of which have updates on weekly/daily bases to keep up with the ever-changing technology they are protecting. Along with these the two-factor authentication has been an important introduction to securing many accounts. You can think of Cyber security only by recognizing the many aspects that it holds

###### **What is likely to be able to be done soon? and What makes it possible?**

According to some the future holds many more regulations introduced by local and state governments to help prevent the risk by standardizing the safeguards that need to be in place. In terms of technology Forbes states (chuck brooks, 2020) the introduction of AI is said to be the future, with the focus on Machine Learning. It is stated that the technology will rely on rapid automation of predictive analytics, which in sense will be the fastest way to identify new cyber-attacks, draw statistical inferences, and push that information to endpoint security platforms. Amongst other key notes I believe the use of AI to integrate SOAR or security orchestration automation and response into a single interface which will allow security staff a faster more accurate way to process the large volumes of data to prevent or stop attacks that may be coming or are currently underway.

Apart from the introduction of AI there is also talks of Biometrics, The world economic forum (William Dixon, 2019) states that there is expert consensus that a three-factor authentication will be the best option ‘Know’ (password), ‘have’ (token) and ‘are’ (biometrics). With this also brings new threats of exploitation, with the use of fingerprints, eye scans, and voice as all these will need to be stored and the more information that is stored the more that can be stolen.

As stated previously there are many safeguards to help in the world of cybersecurity, Current technologies in more detail as listed by Educba (2020).

Data Loss Prevention  
DLP is a set of tools and processes used to ensure that sensitive data is not lost.   
This Validates the data sent from organizations/persons not of a sensitive nature. It scans all outgoing data to ensure it is appropriate and something that is not confidential. Once a violation has been identified, DLP enforces correction with alerts, encryption, and other protective actions. The main reasons for using DLP is for Personal Information Protection/Compliance, IP Protection, Data Visibility.

Intrusion Detection System (IDS)  
This technology monitors all incoming traffic to organizations/persons to ensure that it is not of a malicious context. The main purpose for IDS is to inform IT personnel that a network intrusion may be taking place, it is a passive technology as it only detects notable traffic after the fact and does not block or stop it. Amongst the IDS they also fall into subcategories such as VM-based IDS, stack-based IDS, signature-based IDS, perimeter IDS, and anomaly-based IDS.

Intrusion Prevention System (IPS)  
This technology is a form of software application or hardware appliance that monitors all incoming traffic to organizations/persons to ensure that it is not of a malicious context. The main purpose for IDS is to inform IT personnel that a network intrusion may be taking place, it is a passive technology as it only detects notable traffic after the fact and does not block or stop it. Amongst the IDS they also fall into subcategories such as VM-based IDS, stack-based IDS, signature-based IDS, perimeter IDS, and anomaly-based IDS.

Security Incident and Event Management (SIEM)  
This Technology is that which acts against traffic that is deemed malicious by the IDS. It usually drops the packets of information incoming so they cannot enter the organizations system. The main difference between the IDS and this the IPS is a IPS can access the IT network and protect it from attacks/abuse. It monitors intrusion data and prevents an attack from developing by doing things such as closing access points, configuring firewalls.

Firewall  
The firewall is the first layer of protection on any system or network, it comes in many types depending on the role that is required of it. It makes sure that the internal network is protected from unusual/malicious traffic cannot enter. A firewall can be hardware, software or both. There are also many types of firewalls such as Proxy firewall, Stateful inspection firewall UTM firewall, Next-generation firewall (NGFW), and threat-focused NGFW, there is also the great Firewall of China.

Antivirus  
As name states it indicates a virus and removes it based on a repository of signatures present in the coding. Needs to be kept up to date to keep all signatures on record to detect the newest of threats. What it does is to Scan specific files or directories, Allows you to schedule scans automatically, Allows you to initiate a scan of a particular file or whole data, removes any malicious code detected (or asks to clean file if possible), and shows some statistics on computer health.

##### **What is the likely impact?**

###### **What is the potential impact of this Technology?**

The impact of this development is huge as it has already been seen with the implementation of varying technologies. If it does not keep up with technology being made you could see some science fiction coming to life and even in the smallest sense identifications that can no longer be confirmed.

###### **What is likely to change**

The things most likely to change is further encryption and making items more secure. As we have seen with development over its time the technology has increased and so has the need to secure them. As it is the blueprints that can enable the good and remove the bad from innovation development it will always be the top priority for anything technologically based.

###### **Which people will be most affected?**

Anyone that uses any technology that shares data will be affected by the use of cybersecurity. According to Cybersecurity Ventures (2019) (Steve Morgan, 2019) - it is predicted that the number of humans on the internet will triple from 2015 to 2022 and reach 6 billion, and by 2030 will increase to 7.5 billion. Another key statistic is that hackers attack every 39 secs, on average 2,244 times a day (University of Maryland). So, with the increase in use of the internet and data being stored there will be an increase in people trying to access this data therefore the need for cyber security will also have to increase.

###### **Will this create, replace, or make redundant any jobs/tech?**

According to the Bureau of Labour Statistics the rate of growth for jobs in IT security is projected at 37% and according to Institute of data Australia is currently short of 2300 workers in cyber security, with an expected demand of at least 17,600 additional professionals in the sector by 2026. So, the furthering of cybersecurity will create more jobs in the coming years new ways of protection of data may be discovered and some technologies may become redundant.

**How will it affect you?**

**How will this affect me?**

This will affect me in numerous ways as It will with a lot of others. With the Digital age and the way, a lot of companies are going with online bookings and recorded data we hope that what we input is secure. If cyber security fails to keep up with demand many will lose identities, money and possibly their minds. On a personal note the increase in need is a good outcome as I wish to get into the field of cybersecurity. On the downside to it all unless there are miraculous improvements nothing will ever be 100% secure so the chances that something bad will occur will always be a likelihood.

**What will be different for you?**

The difference it has made for me is that I am always cautious as to what information I have inputted or sent out. It has come to the state that I have made a fake profile and email for those systems that I do not find a necessity however ask for certain information.

**How might this affect members of your family?**

This will affect my friends and family the most as without the study applied to the field they will be at higher risk. I hope a lot of what comes makes it more secure so the use of the internet will not be so much of a risk. I can see as further development of technology occurs the less people may know about it in their later years and if they have no personal interest in IT at all they may not know what puts them at risk. The development of cyber security is just as important to a big company as it is to anyone. The learning curve for how everything is moving even in its current state has been neglected to be taught to the elder generation, so the reliance of programs to automate your security will be the defining factor of how the future turns out.

**References**

Brooks, C., 2020. *4 Evolving Technology Areas Of Smart Cybersecurity*. [online] Forbes. Available at: <https://www.forbes.com/sites/chuckbrooks/2020/07/05/4-evolving-technology-areas-of-smart-cybersecurity/#5050c31668fc> [Accessed 1 October 2020].

Cybercrime Magazine. 2020. *Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021*. [online] Available at: <https://cybersecurityventures.com/cybersecurity-market-report/> [Accessed 1 October 2020].

Data, I., Data, I. and Data, I., 2020. *Is Cyber Security In Demand In Australia? | Institute Of Data*. [online] Institute of Data. Available at: <https://www.institutedata.com/blog/is-cyber-security-in-demand-in-australia/> [Accessed 1 October 2020].

Inside Out Security. 2020. *110 Must-Know Cybersecurity Statistics For 2020 | Varonis*. [online] Available at: <https://www.varonis.com/blog/cybersecurity-statistics/> [Accessed 1 October 2020].

Technologies, S., 2020. *Security Technologies | Top 7 Key Security Technologies*. [online] EDUCBA. Available at: <https://www.educba.com/security-technologies/> [Accessed 1 October 2020].

Wodc.nl. 2020. *WODC | 2956 - State Of The Art Cybersecurity*. [online] Available at: <https://www.wodc.nl/onderzoeksdatabase/2956-state-of-the-art-cybersecurity.aspx> [Accessed 1 October 2020].

World Economic Forum. 2020. *3 Technologies That Could Define The Next Decade Of Cybersecurity*. [online] Available at: <https://www.weforum.org/agenda/2019/06/3-technologies-that-could-define-the-next-decade-of-cybersecurity/> [Accessed 1 October 2020].

www.kaspersky.com.au. 2020. *What Is Cyber Security?*. [online] Available at: <https://www.kaspersky.com.au/resource-center/definitions/what-is-cyber-security> [Accessed 1 October 2020].