IT Technology 2 – Ben Mason

Cybersecurity

**What does it do?**

Cybersecurity covers the area of information technology relating to the protection of the cyberspace being networks, systems and programs from attacks made in the digital world. The purpose of these attacks are usually to obtain, destroy or tamper with sensitive information and data possessed by a company or business. One of the largest motives for cyber attacks are monetary ones where the attackers target banks or similar venues to extort money from users creating an obvious need for cybersecurity in the current digital world. Cybersecurity comes in many forms, not all digital, some of which being technology, people working behind the computers and protecting against live hacks as well as many different processes and protocols put in place to protect a system. The people aspect of cybersecurity can also come down to users and those whom may be the victims of potential attacks. This can be done through creating difficult to guess passwords to protect the users’ own accounts or even simply being careful of which links the user may click on and ensuring they are from trusted sources. These simple and easy to carry out measures while they may not seem as though they are forms of cybersecurity, are one of the most effective forms, stopping the breach before it even occurs. The processes component of cybersecurity revolves around protocols in place to set guidelines and a framework to workaround in the event of a cyber attack whether only an attempted breach or a successful one. These processes can guide you showing how to identify an attack, detect them, respond, protect your system as well as recover from any breaches you have experienced and prevent future occurrences. There are 3 main technologies that must be protected from cyber attacks, endpoint devices such as smartphones and computers, internet accessing devices such as Wi-Fi routers, modems and the cloud as well as all smart devices that may be scattered around the home. Some household technologies that are commonly used as first lines of defence against cyber attacks are basic firewalls, antivirus software and malware protection amongst others. Cybersecurity is becoming increasingly important with the Australian government planning on tripling ‘the size of the sector by 2026, as cybercrime continues to grow’ [1]. The growing trend amongst cybersecurity firms is that cloud computing will become the new top priority in the market as the cloud rapidly takes control over the digital space with more and more people relying on it each and every day. This results in cybersecurity needing to be predominantly focused on the cloud and its protection seeing as it will soon become the largest target for cyber attacks. Along with the growing population and higher percentages of the world having access to the internet and cloud computing comes greater risks for breaches of security in the cloud. This is because when the cloud has more and more users, it becomes under more stress and as such becomes inevitably susceptible to security issues. The cybersecurity industry is struggling to keep up with the exponential demand for cloud based solutions as shown through the high job demand and salary in the sector. This instability in cloud service protection is constantly being worked on and improved upon and will be much more secure in the near future.

**What is the likely impact?**

The impact of a growing cloud cybersecurity sector will be more secure cloud services for all users and a higher level of peace of mind amongst them knowing that they are at less risk of a security breach where all of their sensitive information can be accessed by a hacker. This lessened risk could also be the turning point for cloud based computing as it could be what makes many people who were previously wary of the uses of cloud computing and its safety and would potentially persuade them to try it for the first time. This would achieve the main purpose of cybersecurity which is to provide a safe digital space free from hacks and security breaches. If an increase in cybersecurity in the cloud space would entice more people to reap the benefits from safe cloud based computing then the cybersecurity element of it would be complete. The people who would most be effected would be the group of people who have large amounts of data they wanted to offload into the cloud from hard drives or the like but had their concerns about the safety of cloud computing. This would greatly benefit them and introduce them to the cloud. Another demographic who could be benefited from this is anyone with an online account, this is because all online accounts are stored in the cloud where a user’s password and often email is kept in an encrypted file. These encrypted files however are often the targets of breaches and hence if these breaches were to be lessened then all users of online accounts would be benefitted from a lessened likelihood of having their account details shared with the public and all related personal files. An increase in cybersecurity in the cloud based world could only create more jobs to protect the ever growing cloud space.

**How will this affect you?**

In my daily life I use cloud services to access all of my online accounts and relevant data stored for those accounts including emails and the like as well as for all of my data which I choose not to store on a hard drive with the risk of losing it. I find the cloud is a safer and less costly approach to using a hard drive, putting me in the same demographic as the aforementioned people who would benefit from a cloud world with a higher degree of cybersecurity. Being able to access the cloud securely can increase my confidence in its use and hence allow me to be able to access my cloud information remotely from any location I need to without needing to be concerned whether the internet I’m using at an internet café or the like is secure enough for me to log into my cloud accounts. I am able to have confidence that the cybersecurity behind my cloud accounts can protect and encrypt my sensitive data from any hackers that may be on an unsecured Wi-Fi connection. This can help me to efficiently utilise the many uses of cloud computing being the ability to access it anywhere the user pleases. Without the added security coming in the near future, I would have to be careful of where and when I accessed my cloud accounts, defeating the purpose of cybersecurity. My father has several thousand family photos from his entire lifetime which he had stored on a hard drive up until recently due to the security of the cloud and its improvements over time. Prior to uploading it to the cloud he had his reservations and did not want to risk losing all of the precious and priceless photographs, however due to the growing cybersecurity space in the cloud, those reservations diminished over time, upholding the purpose of cybersecurity.

**Bibliography:**

1. Nest. 2020. The fascinating evolution of cybersecurity – Nest. [ONLINE] Available at: <https://www.latrobe.edu.au/nest/fascinating-evolution-cybersecurity/>. [Accessed 03 May 2020].
2. Cisco. 2020. What Is Cybersecurity? - Cisco. [ONLINE] Available at: <https://www.cisco.com/c/en_au/products/security/what-is-cybersecurity.html>. [Accessed 03 May 2020].