Draft v0.2

**IT Technologies Mara**

**Cybersecurity**

**What does it do?**

Cybersecurity is designed to prevent unauthorised malicious access to IT technology such as networks, programs, devices and systems. Cybersecurity is a multifaceted field of study, which requires that all the different types to work together and function a whole to be affective. Some of the more common parts of cybersecurity will include physical security of key systems, network security, remote logging and monitoring, redundant systems and end user education.

One of the key elements of maintaining cybersecurity is education, because without education of the end user, a sophisticated security system can be easily bypassed. If the end user opens an infected email or falls victim to a phishing attack, a hacker will have instant access to their device. Phishing and ransomware are the leading two biggest forms of cyberattack, and it is costing the global economy in excess of $600 Billion a year. These two forms of attack are based on human error and the only way to strengthen the defense against this is education of the end user. This is a growing field that companies are starting to take a lot more seriously, and this is an area where a lot more development is still needed. Additionally, in conjunction with training, limiting user privileges to restrict the installation of unauthorised software can further minimise the risk associated with falling for one of these attacks. It is also important that strong rotating password requirements are implemented across a company to try and prevent the success of brute force password attacks.

From a network perspective, implementing access control lists, vlans, and subnetting can all be used to segregate a network and in doing so, reduce the risk. By dividing the network up, should a breach occur, the hackers do not have unlimited access to the whole network. Additionally, implementing a VPN and network encryption can increase security by making it improbable that a hacker could reverse engineer the data contained within the packets without knowing the encryption keys.

An often-overlooked part of cybersecurity is physical security. There is an old saying along the lines of, “if they’ve already plugged into the network, you’ve lost the battle”, which is a great summary of why physical security is so important. You could have the best firewalls and encryption available but if a hacker can physically plug into one of your network switches or access an authorised computer already on the network, they will able to bypass all the security measures. This is particularly important in remote branches and data centers where there is a greater chance of unauthorised access. Remote branches tend not to be as secure, as often the onsite staff are not familiar with the necessary security measures and contractors may be accidentally granted access to the IT equipment. Data centers have shared space with many different companies, and any company can grant access to an contractor, meaning no one person knows who should have access to the building. This makes potential intruders difficult to detect as you can’t be sure who has been given access to the equipment rooms, or their intentions. Ensuring that unused ports are shut down and cabinets are locked is a good way to combat this problem and should be standard practice, but sadly in my experience it is not.

Cloud based monitoring and reporting are another important part of cybersecurity, with the aim of early detection of possible threats. If a threat is detected early enough, cybersecurity staff can implement changes to reduce the likelihood of a breach or stop a breach in progress. Through the correct implementation of alerts on network hardware and server software, cybersecurity staff can receive automatic notifications when security risks occur, such as: unauthorised rogue connections (both wired and wireless), eavesdropping/spoofing, and denial of service (DDOS) attacks, to name a few.

Redundancy is good IT practice whether for security or general operations. Specifically from a security standpoint, redundancy allows you to recover from attack more quickly through the use of a backup to recover any lost data. Backup storage can also be used to identify what has been stolen in the event that hackers erase or damage primary storage.

**What is the likely impact?**

Nearly two thirds of people who use the internet regularly have had their data stolen or compromised at some point. In 2019, it was estimated that 1.5 trillion dollars was lost from the global economy to cybercrime. This has a huge impact on the bottom line of governments and large corporations, as the cost to maintain security and recover losses is passed on to the general population through increased prices, fees and taxes. At a more individual level, identity theft can cause significant disruption to people’s lives. When it comes to identity theft, the impact isn’t always financial. Depending on the goal, it could be to discredit someone, corporate espionage, domestic violence or stalking. With current security technology becoming so effective when implemented correctly, hackers will continue to use human-centric approaches such as phishing, malware and trojan-horses, to gather credit card details and personal data. This is the most straightforward way for a hacker to achieve their goals, with a lot of resources and how-to’s available on the internet, and minimal coding experience or knowledge is required. With a 20% increase of ecommerce hacks over the last 12 months, fraudulent credit card activities are going to continue to grow. This has a great impact on the retailer and the individual whose details were stolen, causing financial losses and stress. This will also have an effect on banks who need to constantly improve their monitoring of accounts to better detect fraudulent purchases.

As the increase in hacking and fraud continues to grow, more jobs will be created in the cybersecurity industry. Unlike other areas of IT, such as automation, this field is unlikely to make jobs in other areas redundant, as security is not a replacement for an existing product. The cybersecurity industry will continue to grow to meet the increasing demand.

**How will this affect you?**

The more I’ve learnt about cybersecurity, the more I think it would be an interesting job prospect. Working towards making better code, better algorithms or even AI that could detect potential vulnerabilities and attacks, prior to the need for human interaction will minimize the risk of human error, which is the most common point of failure in a security system.

This has already affected my day to day life, with companies implementing two-factor authentication to increase the security of my accounts. For example, banking sending my mobile an SMS code before a transfer can be made or having to enter in a security code when signing-in to a new Apple device. Steam requires two-factor authentication just to log in, to prevent an intruder stealing product keys from your games. Google now sends security alert emails to your account when logging in from a new device. All new modem now come with a minimum a basic Wi-Fi password and most now require a login to access the GUI. More companies are accepting PayPal instead of credit card payments because of an increase in demand as more people want secure ways to pay online and minimize their risk.

Phishing emails are getting harder to detect at first glance, and more people are falling for them. This affected me as recently as February this year, when my ISP’s web mail accounts were hacked, and the hackers were able to use this password to access many of my parent’s accounts that shared the same password. It took me several days to reset all the passwords to new unique passwords, and to go back through banking records to verify that there were no fraudulent charges.

I know multiple people who have been hacked, and even after experiencing this, people can still fall for the same techniques and scams. As long as people continue to fall for these techniques, hackers will continue to use them. This is a huge problem when dealing with sensitive information and we all need to be vigilant.

**References**

Cisco. 2020. *What Is Cybersecurity?*. [online] Available at: <https://www.cisco.com/c/en\_au/products/security/what-is-cybersecurity.html> [Accessed 10 April 2020].

Cyber.gov.au. 2020. *Home Page | Cyber.Gov.Au*. [online] Available at: <https://www.cyber.gov.au/> [Accessed 10 April 2020].

GBHackers On Security. 2020. *A Rising Of E-Commerce Cyber Attack & Most Dangerous Threats Of 2019*. [online] Available at: <https://gbhackers.com/a-rising-of-e-commerce-cyber-attack-most-dangerous-threats-of-2019/> [Accessed 10 April 2020].

Hashed Out by The SSL Store™. 2020. *The Top Cyber Security Trends In 2019 (And What To Expect In 2020) - Hashed Out By The SSL Store™*. [online] Available at: <https://www.thesslstore.com/blog/the-top-cyber-security-trends-in-2019-and-what-to-expect-in-2020/> [Accessed 10 April 2020].

Itgovernance.co.uk. 2020. *Cyber Security*. [online] Available at: <https://www.itgovernance.co.uk/what-is-cybersecurity> [Accessed 10 April 2020].

Mcafee.com. 2020. *Economic Impact Of Cybercrime Report | Mcafee*. [online] Available at: <https://www.mcafee.com/enterprise/en-au/solutions/lp/economics-cybercrime.html> [Accessed 10 April 2020].

Minute, 2020. *Cybercrime Costs Global Economy $2.9M Per Minute*. [online] Infosecurity Magazine. Available at: <https://www.infosecurity-magazine.com/news/cybercrime-costs-global-economy/> [Accessed 10 April 2020].

PhoenixNAP Global IT Services. 2020. *17 Types Of Cyber Attacks To Protect Against In 2020*. [online] Available at: <https://phoenixnap.com/blog/cyber-security-attack-types> [Accessed 10 April 2020].

Rand.org. 2020. *Examining The State-Of-The-Art In Cybersecurity*. [online] Available at: <https://www.rand.org/randeurope/research/projects/cybersecurity-state-of-the-art.html> [Accessed 10 April 2020].

Technology.org. 2017. *Biggest Cyber Attacks And Their Cost For The Global Economy*. [online] Available at: <https://www.technology.org/2019/07/17/biggest-cyber-attacks-and-their-cost-for-the-global-economy/> [Accessed 10 April 2020].

Us.norton.com. 2020. *Do You Worry About Cyber Safety? Learn Some Smart Defenses.*. [online] Available at: <https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html> [Accessed 10 April 2020].

<https://www.cisco.com/c/en_au/products/security/what-is-cybersecurity.html>

<https://www.itgovernance.co.uk/what-is-cybersecurity>

<https://www.cyber.gov.au/>

<https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html>

<https://www.rand.org/randeurope/research/projects/cybersecurity-state-of-the-art.html>

<https://phoenixnap.com/blog/cyber-security-attack-types>

<https://www.thesslstore.com/blog/the-top-cyber-security-trends-in-2019-and-what-to-expect-in-2020/>

<https://www.technology.org/2019/07/17/biggest-cyber-attacks-and-their-cost-for-the-global-economy/>

<https://www.mcafee.com/enterprise/en-au/solutions/lp/economics-cybercrime.html>

<https://www.infosecurity-magazine.com/news/cybercrime-costs-global-economy/>

<https://gbhackers.com/a-rising-of-e-commerce-cyber-attack-most-dangerous-threats-of-2019/>