Draft v0.2

IT Technologies Mara

Cybersecurity

What does it do? (600 words) What is the state of the art of this new technology? What can be done now? What is likely to be able to do be done soon (say in the next 3 years)? What technological or other developments make this possible?

Cybersecurity is designed to prevent unauthorised malicious access to IT technology such as networks, programs, devices and systems. Cybersecurity is a multifaceted filed of study, which requires the all the different types to be working 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’s higher levels security systems can easily be bypassed by the end used opening an infected email, or falling victim to phishing attacks. 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 weakness and the only way to strengthen your defence 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 those attacks. It is also important that strong rotating passwords requirements are implemented across a company as a whole to try to 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 vpns and network encryption further 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 system, they will able to bypass all your security measures. This is particularly important in remote branches and data centres where there is a greater chance of unauthorised access. Remote branches tend to be not as secure as often the staff onsite are not familiar with security measures and contractors may be accidentally granted access to the IT equipment. Data centres are shared space with other companies, and 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 locket is so important and should be mandatory and commonplace, but sadly in my experience it isn’t.

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 notification 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 backup to recover any lost data and can also be used to identify potentially what has been stolen in the event that hackers erase or damage primary storage.

What is the likely impact? (300 words) What is the potential impact of this development? What is likely to change? Which people will be most affected and how? Will this create, replace or make redundant any current jobs or technologies?

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 affect on the bottom line of large corporations and governments, 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 damage 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 and malware and trojan-horses, to gather credit card details and personal data. This is the most straightforward way to achieve their goals, with a lot of resources and how-to’s available on the internet, while 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 who’s details were stolen, causing financial losses and stress. This will also have an affect 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 is continue to grow to meet the evergrowing demand.

How will this affect you? (300 words) In your daily life, how will this affect you? What will be different for you? How might this affect members of your family or your friends?

The more I’ve learnt about cybersecurity, the more I think it may be an interesting future job prospect. Working towards making better code, better algorithms and even AI that can detect potential vulnerabilities and attacks, prior to the need for human interaction in suspicious circumstances, will minimize the risk of human error, which is the primary 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 SMS codes before transfers can be made, Apple device security coded when signing in to a new device. Steam requires two factor authentication just to logf in, to prevent an intruder stealing product keys for your software. Google now sends securtuy alearts when logging in from a new device. All new modem now come with at minimum a basic WiFi password and most require a login to access the GUI. More companies are accepting Paypal instead of credit card payments and this is because of demand as more and more people want secure ways to pay online to minimize risk.

Phishing emails are getting harder to detect at first glance, and more 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 in excess of three days to reset all the passwords to new unique passwords, and also go back through banking records to verify that there were no fraudulent charges.

I know multiple people who have been hacked, and even knowing people have been hacked doesn’t meant you wont fall for the same techniques yourself. And as long as people continue to fall for these techniques the hackers will continur to use them. This can become a huge problem when dealing with sensitive information for governments and banks, and we all need to be extra vigilant.

<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/>