What does it do? (600 words)

Cybersecurity is the process and practice of protecting IT systems, programs, networks, and various other hardware and software configurations from a digital attack. Such attacks are known as Cyberattacks, the most common of which relate to gaining access to, making changes to or even destroying sensitive information, extorting money from users through ransomware, or just generally interrupting workflow and business processes. Effective implementation of cybersecurity can be quite a challenging task in today’s IT climate as there are many more devices than there are people, and cyberattacks are getting more innovative than they ever have been. A secure approach to cybersecurity will consist of multiple layers spread across all the technologies that need to be protected, i.e. Computers, programs, networks, or data that an individual or organization wants to keep safe. In regard to an organisation, all of the people, processes, and technologies need to complement each other and work together to be able to create an effective defense against cyber-attacks, with a unified threat management system being the best way to accomplish this. As the weakest link of any security system is always the same, being people, there are many ways that an individual can contribute to cybersecurity. These ways come down to users understanding and complying with some basic data security principles such as: choosing strong passwords that aren’t used in other places, being aware of what emails the user is opening and especially being careful that any attachments to an email are scanned for viruses, but most importantly that users are backing up their data regularly and in a multitude of ways, whether that be externally on USB drives or external hard drives, through the cloud, or a combination of both. As no matter how broad, effective, or even how much you or your company pay for cybersecurity tools, the whole project or company can fail if a careless user makes a simple mistake. If a user clicks on an unfamiliar link or opens a suspicious-looking email attachment this could bring about a massive data loss. Technology is a very important part of cybersecurity as it gives individuals and organizations the means and tools to protect themselves. Three main entities that must be protected on a technological level: user endpoint devices such as your computer, phone, and even the way you access the internet such as your modem or router, the user's network itself, and the cloud. Technologies that are common in protecting these entities consist of firewalls, filtering of the domain name system (DNS), anti-malware and antivirus software like Malwarebytes or Windows Defender, and an email security system. Cybersecurity is important and everyone benefits from being more secure in a digital environment. On an individual’s level, a successful cyberattack can result in anything ranging from identity theft or extortion to even losing sensitive data like family photos. The main forms of cybersecurity threats are phishing, which is the practice of sending fake emails that look like they are from a legitimate source that aims to steal data sensitive to the victim such as a credit card number or the user's login details to one or many websites. Ransomware, which is software that is designed to extort money from a victim by blocking access to files or even a whole computer system until one pays the ransom, which does not guarantee that the user will be able to recover everything. Malware, which is software designed to gain unauthorized access or cause damage to the victim's computer, and lastly Social engineering, which is a tactic that cyberattacks use to trick victims into revealing sensitive information, usually resulting in either blackmail or them stealing confidential data.

What is the likely impact? (300 words)

As our society becomes more dependent and reliable on technology, so must our cybersecurity systems change and grow with our usage. Gone are the days of hiding personal information, as a lot of it ends up all over our social media accounts and people even store sensitive information such as credit card or bank details in ‘secure’ cloud services such as Dropbox or OneDrive. This means we have a database of cybersecurity threats that is constantly evolving and changing. As world governments bring more attention to cybercrimes and bring in solutions like Europe’s General Data Protection Regulation (GDPR) threats such as data breaches can be held more accountable. GDPR forces all organisations that operate in the European Union to communicate these data breaches when they happen, assign a person in the organization as a data protection officer, anonymise user data for privacy and most importantly require users to have to consent to their information being processed. Being complacent with cybersecurity can have many impacts on a user or organisation. From economic impacts like the theft of intellectual property and corporate information, the general disruption in trading while an organisation tries to recover from a data breach, and even the cost of having to repair systems. Reputational impacts, the breach of trust that a consumer may feel and choose to go with a different service and being slandered in the media. To regulatory costs such as fines or even sanctions for breaking data breach laws such as GDPR. A few examples and consequences of cyberattacks and data breaches include:

• Equifax – Equifax suffered a cybercrime identity theft event that affected approximately 145.5 million US consumers, 400000-44 million British residents, and 19000 Canadian residents. As a result of this breach, Equifax shares dropped 13% and numerous lawsuits were filed against the company. Equifax agreed to a settlement that consisted of $300 million for victim compensation, $175m for states and territories affected, and $100m in fines.

• eBay – eBay was the victim of a data breach targeting encrypted user passwords between Feb and Mar 2014, which resulted in the company asking every single one of its 145m users to reset their passwords. The attackers used a set of employee credentials to access this password database. As well as passwords, the database also included information such as names, email addresses, dates of birth, phone numbers, and even the physical addresses of the userbase. eBay disclosed the data breach in May 2014 after a month-long investigation.

How will this affect you? (300 words)

Cybersecurity and privacy affect my daily life immensely, I am constantly checking databases to see if any personal information of mine has been breached. I visit both Privacy Tools and Prism Break regularly to find new ways to protect myself from digital threats and to inform friends and family of better ways that they can protect themselves. Even going as far as looking into hosting my own cloud service on my home network through Nextcloud to prevent the possibility of any sensitive information being in an unsecured cloud service such as OneDrive or Dropbox. I used to run a multitude of antivirus, malware and spyware software on any computer I would touch but have since come to realise the best combination of security software, at least for my needs and usage, is simply a few browser extensions: uBlock Origin, HTTPS Everywhere, Decentraleyes, ClearURLs, and Firefox’s built-in containers; Windows’ built-in antivirus software Windows Defender, a bi-weekly scan of Malwarebytes and most importantly common sense, which is the hardest thing to try and teach friends and family members about when it comes to online safety. A few examples of common sense regarding cybersecurity consist of avoiding piracy wherever possible, as fake programs are one of the biggest ways that people end up with virus’ and the like, avoiding suspicious websites with 10 different ‘download now!’ buttons and avoiding the use of logging in and making new accounts through social media links such as Facebook and Google. These simple measures can help ensure that one can feel extra safe personally regardless of the user’s confidence in the service they are attempting to use. Another huge part of keeping myself protected on the internet is using a password manager. I originally used LastPass for the longest time as I felt paying for the service would make sure that it was extra secure and that the money they received from their userbases subscriptions per month would go into adding extra layers of security. I ditched LastPass as soon as I heard that even they had a data breach and moved on to hosting my own password manager through KeePass and hosting the database on Dropbox so I had access to it on any device I needed to use. Realising Dropbox probably is not the best place to store such secure information I have now moved onto Bitwarden which at least for the meantime is everything I need out of a password manager.

References:

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

Cisco. 2020. *Cisco Umbrella's Top 10 Cybersecurity Tips - Cisco Umbrella*. [online] Available at: <https://umbrella.cisco.com/blog/cisco-umbrella-top-10-cybersecurity-tips?utm\_medium=web-referral&utm\_source=cisco&utm\_campaign=cs-fy2020-q2-cisco-100-day-sprint&utm\_term=pgm> [Accessed 10 July 2020].

Upguard.com. 2020. *Why Is Cybersecurity Important?*. [online] Available at: <https://www.upguard.com/blog/cybersecurity-important> [Accessed 10 July 2020].