Cyber security is the protection of computer systems and networks from theft or damage to hardware, software, or electronic data. This is important to everyone’s lives ranging from the person who just got their first computer all the way to the giant companies relying completely on their technology (Cisco, n.d). The cybersecurity industry is rapidly advancing all of the time and already has many new and significant advances since the industry first began in 1972. Currently the Cisco Adaptive Security Appliance holds the throne as the state of the art technology used in cyber security. It’s features include integrated Virtual Private Server, Virtual Private Network, antivirus, antispam, content inspection capabilities, multi-node and automated clustering, enhanced productivity and performance, all devices can be connected via a secure and efficient network, secures IP addresses and data centers (Cisco, n.d). It also builds upon regular firewalls which monitor the network traffic on a system or network and determine whether it can get through or not (Cisco, n.d). You can picture it like a security guard letting people into an event, usually they make the right call but sometimes someone may get in who has no business being in there. This raises a major issue because usually by the time someone realizes there is a problem their files could be gone, system destroyed or even their identity stolen. Such as happened in 2017 when the credit reporting agency that assesses the financial health of most people in the United States Equifax had a data breach. This breach led to hundreds of millions of people having their personal information stolen and it was attacked in a vulnerable web portal that was never fixed due to their internal processes. The breachers went from this web portal to other servers because they were not configured properly which then allowed for them to retrieve all of the usernames and passwords of all existing clients without difficulty and continue on this data theft. Equifax was unaware of the breach for months because they did not renew an encryption certificate on one of the internal security tools and after that they did not make the breach public until over a month later ([Fruhlinger](https://www.csoonline.com/author/Josh-Fruhlinger/), 2020). A question that came out of this is how the industry can notice those small disguised threats sneaking their way into your system to cause major problems. Right now it is up to automation and humans to find out about these breaches and then act on them, however the industry will most likely turn to artificial intelligence in cybersecurity defenses to assist in rectifying these issues (Parker, 2020). Right now they create more of a cybersecurity risk than a reward because when new technology is released the potential corruption is not fully known and is only determined the longer a system has been released for and how hackers try to find the vulnerabilities within the new systems. However, on the plus side for early AI use it can automate and compute faster than a human can, which will then allow for the possible corruption points when acted upon by an outside user or when noticed by an AI to be fixed much faster than by waiting for an actual person to notice it. It would also be more beneficial to bring it out sooner than later so that the issues with using artificial intelligence can be highlighted earlier on in the process of using it as opposed to trying to work out every single little kink just to find out it is still full of holes.

Continuing on, due to this current technology systems will be at less of a risk of being hacked and will allow for new technology to be fixed quicker than ever before. What is the downside of this? Well the problem here is that those looking to cause harm to one’s systems or devices will also be able to use artificial intelligence to try and wreak havoc on those same systems or devices. Those individuals will most likely use one of two options. They will either hack into the AIs that are being used and use those to steal information and cause havoc, or they will create separate AIs that solely have the intention of causing malicious corruption (Ramachandran, 2019). This also poses a problem for technology that does not have up to date cybersecurity software on it because as the opposing side gets stronger it will be much easier to be hacked into due to the lack of strong security. Situations such as the Equifax data breach was caused by a lot of human error that eventually led to this breach. Human error would not be an issue if it was being done by AI. Using Artificial Intelligence will affect everyone who uses technology. It will make newer technology more desirable to consumers for the updated security that will come with it. It will also save companies money because the AI can go through all data faster and more thorough than a human could (Balbix, n.d). It will not necessarily make any jobs redundant nor will it create new ones, but it would allow for those formally tasked with going through the data to focus more on other tasks such as upgrades to the AI or allow them to focus more on fixing the problem rather than spending time looking for these errors or breachable points. This will cause the cybersecurity industry to rapidly advance because people will be focusing solely on how to make things better, not fixing current mistakes.

In conclusion, even with this major upgrade to cybersecurity, it will most likely not affect my life or my friends and families lives very much. This is due to the fact that cybersecurity is at its best when people are unaware it is happening. If people need to become more aware of cybersecurity that would mean that it is not entirely able to do its job properly and has been hacked. People do not know they have a problem with cyberthreats until they break through their cyber security and notice corruptions happening in their systems or devices. If cyber security is somehow increased to the point where hackers are unable to pass through it no matter what they do then people will no longer become aware of threats and problems and forget that cybersecurity is even a thing. Now, will that ever happen? The short answer is no, that is impossible. It is impossible to build up cybersecurity that strong because anything that is built can be used against those creating it as they do not fully understand it and hackers can exploit that lack of knowledge that exists. This is typically why many games, devices or programs released have an update very shortly after being released. Someone has found how to take advantage of a small window that the developers/creators did not even know existed. Changes in cybersecurity will have neither a positive nor a negative impact in my life because as the industry is constantly evolving the opposing side is too. With this in mind we wonder when the end of the battle between cybersecurity and cyberthreats will end, especially with how deeply involved everyone is with their technological devices.

Balbix n.d, *Using Artificial Intelligence in Cybersecurity*, Balbix, viewed 16 January 2021,

<https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/#:~:text=In%20security%2C%20AI%20can%20identify,detect%20intrusions%20before%20they%20start>.

Cisco n.d, *What is a Firewall?I*, Cisco, viewed 16 January 2021,

<https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>

Cisco n.d, *What is Cybersecurity?*, Cisco, viewed 16 January 2021,

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

Field Engineer n.d, *What is the Cisco Adaptive Security Appliance (ASA)?*, Field Engineer, viewed 16 January 2021,

<https://www.fieldengineer.com/skills/cisco-asa>

Fruhlinger, J 2020, *Equifax data breach FAQ: What happened, who was affected, what was the impact?*, CSO, viewed 16 January 2021,

<https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html>

Parker, J 2020, *What is the future of cybersecurity?*, Future US, Inc., viewed 16 January 2021,

<https://www.techradar.com/news/what-is-the-future-of-cybersecurity>

Ramachandran, R 2019, *How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks*, Entrepreneur India, viewed 16 January 2021,

<https://www.entrepreneur.com/article/339509#:~:text=Further%20advancement%20in%20AI%20can,or%20device%20has%20been%20affected>.