**CYBERSECURITY**

**The welcoming to Cybersecurity**

Cybersecurity has multiple layers of protection spread across computers, networks, programs or data that intend to keep people and their files safe. Within an organization, it is incredibly important to insure that the people, processes and technology all complement each other to create an effective defense from cyber attacks. Users need to understand and comply with the very basics of data security. This can be in the form of selecting strong passwords, being cautious when opening suspicious emails and of course backing up their own data. Cisco has 10 principles that they preach to help businesses fight against attacks.

**Cisco’s principles**

1. Realize that you are a potential target for hackers. Don’t live a dreamland where you believe it wont happen to you, it does.
2. Ensure that passwords are strong Use a strong mix of characters
3. Never leave your devices unattended
4. Be careful when clicking on attachments, especially in emails
5. Banking online, or shopping online should be done on a device that belongs to you and on a network that you trust
6. Backup your data, antiviruses are also always good to have
7. Be mindful on what you plug into your computer
8. Be careful with what you post on social networks
9. Be cautious when giving sensitive information, even offline through phone calls
10. Monitor your accounts and look out for suspicious activity

While Cisco’s principles are appreciated and may help, we should look back and see what security measures we once had and how they have developed. When reading this information keep in mind that the demand for cybersecurity will constantly be increasing throughout the years while our society slowly but surely turns to technology. Consider this, while we once stored ‘files’ in a file cabinet, we are now storing ‘files’ in a cloud. The sensitivity of these files will change throughout organization, but the security of these files is nonetheless important. While these fails were once protected with a physical key. We need to look to cybersecurity to create virtual keys to keep our files and sensitive data locked and secured from attackers.

**Utilizing Cybersecurity**

A company from Israel has developed a new form of cyber security that they have described as ‘moving target security’. The concept behind moving target security is that the security scrambles the names, references and locations of files in the server’s memory, as well as the application itself. This makes it a lot harder for malware to infect a system.

A familiar cybersecurity measure that we would all be used to by now comes in the form of firewalls. This concept is not new however, advances to firewalls have now been implemented. The industry leader is Fortinet. Fortinet have developed a firewall to protect websites and web apps from virus, ransomware and malware infections while preventing intrusion from hackers and blocking distributed denial of service attacks.

**The challengers of Cybersecurity**

The current state of the art technology in Cybersecurity was researched by an organization named RAND Europe which was commissioned by the Netherlands Research and Documentation Centre (WODC) on behalf of the Dutch national counterterrorism coordinator (NCTV) They found that one of the key reasons to why advances in Cyber technology is hindered is due to the constant knowledge and research gaps that are often found. Legal and ethical concerns also hinder the growth but it is arguably understandable due to the fear that technology may be advancing too quickly.

Within the next 3 years, we will see the need for technology to keep advancing, this inherently means that cybersecurity also needs to keep advancing to keep up with protecting ourselves from the other advances in technology. For example, the advances in artificial intelligence will require heavier cyber security for us to ensure that we are always in complete control of situations when dealing with AI.

**Advances in Cybersecurity**

There has also recently been advances in cyber security through the form of ‘Blockchain’. The threat from cybercriminals is constantly increasing, this means that security needs to increase with it. Blockchain is a security apparatus. Which in plain terms is just a bunch of blocks and chains. When we look deeper into it though the genius of it becomes obvious. Blocks store information about transactions like the date, time and purchase price of something. Blocks store information about who is involved in transactions. However, instead of using your actual name, the purchase is instead recorded without any identifying information, using a unique ‘digital signature’ which works very much like a username. The use of blockchain is most prevalent when looking at cryptocurrency.

Advances in artificial intelligence will be the area that impacts society the most. It will reinvent cyber security as a whole. Not only will we need to develop cyber security measures to protect us from AI malfunctioning, but we can even use AI as a tool of cyber security. The impact of these advances could honestly mean a loss of jobs for a lot of people. Jobs that require manual labour would be the first to go as AI would be able to do the same job and potentially more efficiently. For example, security guards have 2 major responsibilities, observe and report. AI could do the exact same thing and wouldn’t require food or a wage. Yes, there are upkeep costs involved but as technology becomes more advanced and we find a better way to fuel AI, the cost to reward ratio may even become worth it for some organizations. Another area that will be heavily affected are our supermarkets. Staff that restock shelves will have their jobs on the line since AI could do the same thing, and again, more efficiently. We have already seen this happen in our supermarkets through the implementation of self-service machines. This is a form of AI that we now consider to be a normal part of society.

**The affects of Cybersecurity**

Coming back to my main topic, the development of cyber security will also allow for a more proactive defense against attacks. The benefits of Artificial intelligence based cyber security will mean that they can work around the clock without breaking a sweat or wanting a break, they can respond within milliseconds to cyber attacks that could take even months for humans to identify. There are many benefits that AI technologies will have on cyber security, but there are also some negatives. AI can also be used to attack which would mean new forms of attacks that we may not ready for. AI-based solutions can be expensive and training to operate the AI may be more challenging for the average person to operate.

The advances in cyber security will affect me as I will need to become more aware on how to fight against cybercriminals. As the world sees advances in cyber security, we will also see more attacks on our technologies. A very important technology that we all use everyday is the mobile phone. This small device holds some of our most personal information. I can nearly guarantee that majority of mobile uses don’t even have an antivirus on their phones. As we advance in technology, I bet that one day it will become a new norm for myself and friends and family to consider an antivirus on mobile phones as an essential part of owning a mobile.