The History And Concept Of Cybersecurity

Virus, malware, ransomware, phishing... What is all this? Where did it come from? Why do we even have this? In 1989, the birth of one of the deadliest and unwanted disease for a computer, the first worm was created by Robert Morris (Julian, Ted, and CMO). Robert Morris was on a mission to determine the magnitude of the internet. In order to find out what he was looking for he used a known bug and used the unix platform to push his program to replicate it across the networks and allow it to keep replicating itself (The History of Cyber Security). Little did he know how deadly this would be. This self replicating virus spreaded through the internet so aggressively and rapidly that it had affect the internet greatly (The History of Cyber Security).

The internet slowed down at a very unexpected rate and had untold damages that were not expected (The History of Cyber Security). This known bug is recognized as the worm or as the Morris Worm, which had effects that was beyond slowing down the internet. This implementation of the worm recognized Robert Morris as the first person to be charged under the Computer Fraud and Abuse Act. He however gained recognition for this and is now a professor at Massachusetts Institute of Technology (MIT) (The History of Cyber Security). The Morris worm and the unwanted attacks that followed were the early stages of having to deal with cyber-security attacks. This was just the beginning of the whole havoc of cyber-security attacks. This action of Robert Morris led to the creation of the Computer Emergency Response Team. The Computer Emergency Response Team is a nonprofit research center for systemic issues that affect the internet (The History of Cyber Security). The Computer Emergency Response Team, also known as CERTs, coordinate responses to such emergencies like the attacks that can cause a disruption in the internet and other networks (Julian, Ted, and CMO).

From the 1990s viruses went viral, and they were all over the headlines. The ‘ILOVEYOU’ and Melissa viruses infected millions of Personal Computers, which caused the failure of email systems all around the globe (Julian, Ted, and CMO). All these strategies were for a financial motivation. Such threats developed the antivirus technology. The function of the antivirus technology is to identify the signature of the virus and to prevent it from executing. These viruses and threats made all computer users aware of the risks of reading emails from untrusted sources and prevent them from opening such emails and their attachments. (Julian, Ted, and CMO) From one Morris worm to so many viruses and threats that the internet and other networks possess, that now people need to be more cautious about what they do and where they store their data. All of these actions of cyber attacks led to one thing, a great deal that every individual and every organization need to take seriously, because there is no end to all these attacks, known as cybersecurity. According to cisco, “cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These attacks are usually

aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes" (What Is Cybersecurity?).

Cybersecurity not only affects an individual, but also affects a business or an organization. Any motive can lead an individual to program and create a virus or threat to any other individual or business, it is not necessary for it to be for financial motives (What Is Cybersecurity?). However, most cases today are because of financial motivation or for stealing someone's identity to be able to perform an illegal act so that they, the person actually performing the illegal act would not be caught. Attackers today are finding many innovative ways to attack technologies and target the innocent ones. This makes it very challenging to implement the most efficient and effective cybersecurity as there are more devices than people (What Is Cybersecurity?). Cisco explains how a successful cybersecurity will have multiple layers of protection. This multiple layer of protection will be spreaded out in a computer, network, all programs and data that one wants to keep safe from being attacked from virus. To create an effective defense from cyber attacks, an organization, the people, processes and technology must all complement one another. (What Is Cybersecurity?) To avoid any kind of cyber attack, users must recognize the importance of and comply with the general data security principles (What Is Cybersecurity?). One must choose a strong passwords, they must be aware of and be cautious of attachments in emails, and not just open any attachments (What Is Cybersecurity?). One should always backup their data. There are many password generators that one can use to be able to generate a strong password to avoid anyone from hacking their accounts. One can start to notice how password requirements are not becoming more stringent. You need to maintain a uppercase, lowercase, alphabetic, numerical, and special characters. Now passwords have an expiration date. A lot of login passwords are only valid till a certain time period and one needs to change the password. This encourages people to change their passwords to avoid any attackers to target them. Organizations and individuals both need to be able to deal with attempted and successful cyber attacks, and to do so, they must have a framework (What Is Cybersecurity?). A very strong framework can guide you through to avoid cyber attack as much as possible.

National Institute of Standards and Technology, also known as NIST, is the nation's one of the old physical science labs (What Is Cybersecurity?). They have been publishing computer security standards and guidelines for decades and now they have innovated a new cybersecurity framework. The cybersecurity framework allows organizations to tackle cyber risks in a cost-effective way by providing a common language to talk about cybersecurity, and reference best practices around the world. With the cyber threats that are growing in numbers and sophistication today, it is highly important and efficient to have a cybersecurity framework that brings cyber risks down to a satisfactory rate. (What Is Cybersecurity?) The following three main technology related entities that must be protected are the devices like computers, routers, smart phones and other smart devices; networks; and the cloud (What Is Cybersecurity?). Technology is the key to giving organizations and individuals the cyber security tools that is

required to protect them from cyber attacks. The technology used to protect these entities require one to reply on DNS filtering, malware protection, antivirus software, next-generation firewalls, and email security solutions. (What Is Cybersecurity?) These technologies are highly required to be downloaded into each organization or individuals computers to allow their devices and their networks to be safe and protected from malicious attacks that may be posed by an attacker. These technologies continuously run and scan for any unwanted or suspicious viruses that the devices may have or any new content downloaded will be scanned to see if it is not a virus. This will alert the user the possible threats that they have or can lead, and will help the user delete any unwanted suspicious threats or viruses. In today's world everyone uses technology. Technology basically rules the world right now. No one can survive a day without technology. This advance piece of software or hardware was created to help us function and perform tasks at a faster and efficient rate. Technology is suppose to help us excel with almost everything we do, however, it can also take away everything from us. Just one simple attack towards these advanced performing technology that goes unseen can cause us more than what it gives us. Absolutely any technology, software, or hardware can be hacked or attacked with an unwanted malicious virus. Advanced cyber defense programs can benefit everyone from being compromised with an attack (What Is Cybersecurity?).

Identity theft, blackmail attempts, loss of important data from a high level confidential document to as simple as a middle school assignment can be compromised to a cybersecurity attack. Attackers would attack an individual as well as a organization. No matter how small or big an organization is it can also be compromised with a cybersecurity attack. Organizations like hospitals, small businesses like an architectural firm, or even a high level security offices for the government, or government data files can be attacked with such malicious virus. One can only imagine what would happen if the government data files where attacked and all the individual and high profile database was leaked. What kind of problems would that lead to? Anything confidential would now be in the hands of every public. This means the government and the country would have been compromised and other countries who are enemies of the country would now have those data files.

People would not trust the government anymore. They would feel that all their confidential data is now out to the public and their lives and identity would be at stake, easily for another attacker to attack them. This could cause a chaos in the country and people would question the government. Therefore it is highly important and beneficial to use cybersecurity to help prevent unauthorized malicious cyber attacks, data breaches and identity theft and it can help aid in risk management (Margaret Rouse). One of the most challenging elements for cybersecurity is that the security risks is constantly evolving. Another challenge that one would pose would be to keep up with the growing technologies, security trends and threat intelligence. There are multiple forms that a cyber threat can be proposed in. Ransomware, social engineering, and phishing are some of the possible forms of cyber threat. Ransomware is a malware or a group

of malware that locks or encrypts system files in the victim's computer (Margaret Rouse). Typically the attacker would demand for payment to decrypt and unlock the system files on the victim's computer. Attackers behind the ransomware attacks usually demand payments in virtual currencies like the bitcoins (Admin. What Is Cyber Security All about?). This specific demand keeps the hacker from being tracked down by the law enforcement. Ransomware infects the computer through malicious email attachments, and website links (Admin. What Is Cyber Security All about?).

One should be very careful and cautious of what emails they open and what attachments they download. Any website links that are sent through a mass message through apps or other emails, should be opened only if you know the source. Certain apps and softwares now come with malicious ransomware that you should be careful when downloading. Social engineering is an attack that trick users into breaking security procedures. This type of attack relies on human interaction (Margaret Rouse). An example would be when you want to stream a video from a website or download something from a website that is usually not trusted, they request you to either disable your antivirus application or to limit your firewall. In some cases they request you to disable any extension that may be installed for your computer's security. If you do not disable what they ask you to then they will not grant you access to the video link or anything that you may be wanting to download. This lures in a lot of people as people are desperate to watch a movie or a show that is available on unsecured sites and the only other place the content is available on is on a paid application. This is when people disable their security and this allows direct human interaction to let in all the possible cyber infections. Another type of a cyber threat would phishing. Phishing is a type of a fraud performed through fraudulent emails(Margaret Rouse). These fraudulent emails look like they come from a reputable source (Margaret Rouse). They mask their emails to look like they are from secured companies or sent from secured vendors.

The purpose of these masked emails are to steal sensitive data like credit card information or login information (Margaret Rouse). Phishing attacks are usually dependant on social networking techniques that have been applied to their emails. Other forms of phishing would be from other electronic communications methods like direct messages sent from social networks like facebook, or even SMS text messages. (Margaret Rouse) Phishers, who are known as the cyber attackers, would also use social engineering to track the victim's feed and activities (Margaret Rouse). They would use the extent of social networks like facebook, Twitter, LinkedIn and other social medias to gather as much as information as possible about the victim. This is why it is encouraged for people to keep their personal life and other information about themselves away from social media. Social media is a great platform to connect with people globally, however, what you share and what you do on those social media sites are all tracked. The phisher masks his emails to look like it is sent from a known contact or organization. This email would carry a malicious file attachment that contains phishing software, or it can present a

link that is connected to a malicious website (Margaret Rouse). It is can be hard for one to tell if it is fake or real. However, there are some emails that are so easily identified as they were phishing for your content and access to your information.

There are many malicious attacks and cyber threats that one can face. There are millions of people that are victims of those attackers, and this isn't going to stop. However, victims are now recognizing the malicious attacks that are coming their way and find a way to not fall in a trap, but the attackers are finding more innovative ways to catch their big fish. Along with so many malicious attacks, there are teams out there that research and run organizations geared towards saving people their personal possession, their identity and other forms of confidential and secure data. The study of cyber security can go down different streams however a good cyber security strategist would take in account of all aspects of security. There is network security, cloud security, application security, and Internet of things (IoT) security. There are no limits to security with this fast pace world that keeps growing with technology.