5-2020

Cyber Security’s Influence on Modern Society

Nicholas Vallarelli

Cyber Security's Influence on Modern Society

Nicholas Vallarelli

B.S. Computer Science

Dr. Francis Parisi

Seidenberg School of Computer Science and Information Technology

Thesis Presentation: May 6th, 2020

Graduation Date: May 20th, 2020

Abstract:

The world of cyber security is evolving every day, and cyber-criminals are trying to take advantage of it to gain as much money and power as possible. As the Internet continues to grow, more people around the world join the Internet. The purpose of this is to see how much of an importance cyber security has and how cyber-criminals are able to utilize the cyberworld for their own personal gain. Research has been done on how the cyberworld got where it is today. Additionally, individual research has been done in an effort to learn how to hack. A hack lab has been created and a study has been done to see if it is possible to hack into a cell phone within one month without obtaining any knowledge prior to the start of the study.

Table of Contents:

Introduction:

What even is cyber security? Cyber security is the defense system put in place to protect from an incoming cyber-attack. These attacks can vary in intensity, ranging from damaging hardware systems to outright destroying those systems, which greatly weakens a computer and leaves it susceptible to an onslaught of cyber-attacks from multiple angles. In order to keep as many of these attacks at bay as possible, these cyber security systems must be built, protected, and maintained. Unfortunately, not everyone understands the true value of keeping cyber defenses up to date. If these systems fall too far behind, it is easy for a powerful attack to blow right through the unprepared defense. After all, one of the best offenses in any scenario is a good defense.

Why is cyber security so important? If there was nothing in place to protect a computer, then any person off the street would be able to infiltrate the computer. Take that example and put it in a much larger setting. For hypothetical purposes, say that Apple, a company almost worth a trillion dollars today, loses all of its defenses mysteriously one day. What would be the result of that? If people found out that Apple suddenly became unprotected, they would obviously be able to rob the company blind. Considering that modern technology involves storing a lot more personal belongings online than in the past, including money, it would not be difficult for this feat to be accomplished. The purpose of this is to explain to people that cyber security is one of the most overlooked necessities in modern society, as not everyone cares about it enough to be able to ensure that they are not hacked. Since a lot more is done online now compared to the past, making sure everything is up to date and fresh is key to ensuring everything is protected.

More measures need to be put in place to persuade people to take better care of their own belongings. Additionally, more measures need to be enforced so that companies can utilize cyber security to its maximum effect. These solutions are out there but said solutions need to be explored in much more detail.

Background:

Technology has evolved very rapidly over the last 80 years. It is important to understand the history of computers and how they have evolved to suit the market and consumers. The first programmable computer was created all the way back in the mid to late 1930s and more advanced computers keep being produced on a regular basis. The most remarkable invention that would shake the computer world forever is the internet itself. The internet, then known as Advanced Research Projects Agency Network (ARPANET), was created in 1969 and was used to connect four universities in the United States, those being the University of Utah, the University of California Los Angeles (UCLA), the University of California Santa Barbara (UCSB), and the Stanford Research Institute (SRI). ARPANET was owned and funded by the U.S. Department of Defense and would continue to be owned by them until 1984. Eventually, people at UCLA got together in order to test the effectiveness of ARPANET, so they attempted to send a message to the computer at the SRI. The message they attempted to send was the word LOGIN. However, only the L and the O were sent successfully before the computer crashed. ARPANET continued to grow in the United States, eventually reaching out to Harvard and the Massachusetts Institute of Technology (MIT). By 1983, more support was needed in order to reach out even further in the world. This led to the creation of the Transmission Control

Protocol/ Internet Protocol (TCP/IP), which is a system that allows two computers to communicate with each other more efficiently. Finally, in 1989, computer scientist Tim Berners-Lee created the World Wide Web that is still in use today. The World Wide Web has gone through multiple changes and updates as well in order to ensure that it stays strong and up to date. The three base components of the internet, while a bit dated in the present time, are still very influential in the continuation of the technological age.

After Berners-Lee created the World Wide Web, he needed to figure out how to spread the internet's influence. He immediately got to work creating three major components of the internet that are still relevant today. Those three components are HyperText Markup Language (HTML), the Uniform Research Identifier (URI), and the Hypertext Transfer Protocol (HTTP). HTML is a programming language mainly used for formatting that is commonly partnered with Cascading Style Sheets (CSS) and JavaScript in order to build webpages, CSS is the language used to style a webpage, and JavaScript is the primary programming language of the internet. The URI, or URL as it is called today, is what is used to identify each webpage as unique. The HTTP is what allows a person to retrieve a link they want to use. The internet has held a massive influence on society for nearly three decades now, and that influence is not going to go away anytime soon.

However, the Internet has not been completely used for good purposes. After people eventually learned the programming languages necessary to contribute to the advancements of the cyber world, a certain group of people rose up and tried to use their newfound power for their own purposes. Those people are known as hackers, and it's important to note that there are three types of these hackers. These three types of hackers are white-hat hackers, black-hat hackers, and grey-hat hackers. White-hat hackers are people who hack for good. This type of hacker usually hacks for either for experimental purposes or for assisting others with their problems. This form of hacking is completely legal and is the most positively received due to its ability to help other people work out problems in their systems. A job commonly associated with white-hat hacking is penetration testing, where a person is hired by a company to hack into their system and report bugs and other holes in the code. On the contrary, black-hat hackers are the ones who do not hack for what is right. Instead, they hack for their own malicious purposes. This type of hacker can attack in multiple different ways, one example of which is known as a Destructive Denial of Service (DDoS), which is when several computers try to access a webpage at once in order to force it to go offline. A computer under a DDoS attack will keep trying to send information to each computer trying to enter the system, but if there are too many it will overload and crash. Other methods of black-hat hacking include but are not limited to writing malware and stealing important data. Unlike white-hat hacking, black-hat hacking is completely illegal. Grey-hat hackers are a bit more complicated. Instead of hacking for just good reasons or just bad reasons, grey-hat hackers may hack for reasons that are both unethical and illegal but are not as dangerous as black-hat hackers. An example of a grey-hat hacker could include someone who white-hat hacks out in public but black-hat hacks when they are alone. Another example of a gray-hat hacker is someone who would spot a vulnerability in a system, but exploit it for their own gain before alerting the person in charge of the system. These types of hackers are more mysterious than the other two types but are more frequently associated with black-hat hacking because they are still breaking the law by exploiting the vulnerabilities in a system and not doing the right thing, which would be to report the issue. Even though they are not as bad as the black-hat hackers, they are still associated with them because they frequently enter a computer system without being given permission to do so.

Hacking will always involve technology, but it can be done through other means, too. As new forms of technology are created, even more people gain interest in hacking into them. One of the more well-known types of hacks is when ATMs are hacked into to obtain as much money as possible. ATMs can be hacked into much faster compared to other types of technology. All that is needed to do this is a small computer that can be placed inside the ATM. By doing this, the ATM's software is bypassed entirely, and money can be withdrawn undetected. After laptops were invented, people found ways to see what a person looked like by hacking into their camera. If the camera gets hacked into, the hacker could record what the other person was doing and use that footage to blackmail them into doing something for the hacker that they do not want to do. Not only that, but with the creation of social media sites such as Facebook, Twitter, and Instagram, came many new ways for people to be hacked. If one of these sites gets broken into and personal information is on them, it can quickly spell disaster for the person who got hacked. For instance, when Cambridge Analytica ended up acquiring and releasing the personal information of several million people, they faced immediate controversy. They were forced to go defunct because of their actions, as they did not get permission to use the personal information from those people affected. Hacking is a problem that is not going to go away, but efforts to push against it are certainly feasible and can be done if enough work is put into figuring out solutions.

One industry that has been hit hard by cyber-attacks time and time again is the cryptocurrency industry. After bitcoin surged in value, many companies were formed in order to assist people who had a lot of them. Typically, bitcoins would be held in a hot wallet, or a type of software that allows cryptocurrency users to store, send, and receive tokens that can be exchanged for bitcoin or other similar cryptocurrencies. However, these types of wallets are connected to the internet and are thus susceptible to being hacked. For wallets to be secured, cold wallets should be used instead. Cold wallets are not connected to the internet and are thus safe from hackers. While cold wallets do offer much better protection against hackers due to the fact that they are not connected to the Internet, cold wallets are not very useful when conducting transactions, hence why hot wallets are much more frequently used. Due to the sheer amount of money being handled by these companies, the cryptocurrency industry has had many different types of cyber-attacks planned and executed against them. Some of the most impactful types of attacks that can occur include phishing scams, exit scams, inside jobs, and 51% attacks. Phishing scams are when someone sends out an email with a link that will infect that computer with malware. If it is clicked, the computer will be infected within seconds and the person who sent the email will be able to control the computer that opened the email. This type of scam is especially dangerous if a company that is worth a lot of money gets attacked. If this happens, millions of dollars can be lost easily. An exit scam is when a company disappears after collecting a large amount of money. An exit scam may occur when the CEO of the company feels like they no longer need the rest of the company and have made a sufficient amount of money. When this happens, they will simply take their money, walk away from the company, and live life elsewhere while the company crumbles. An inside job is when an employee turns against the company and attacks it from the inside. Inside jobs are not often discovered right away since the employees on the inside are not usually suspected first. If the company saw that an employee broke into their security, they might assume that the employee had been hacked first. However, if they are able to find out that the employee was not hacked and willingly infiltrated their systems for their own gain, then they would need to take appropriate action against the treasonous employee. A 51% attack occurs when hackers take over more than half of a network, allowing them to control it. This type of attack occurs frequently in the cryptocurrency industry when an attacker wants to take part in an action known as double-spending. Double-spending is when an attacker tries to make an illegal transaction and then uses the 51% of the network they now control to make the transaction happen twice instead of once, gaining double the amount of money from their attack. There are many different types of attacks that can happen, and it is crucial to be educated on every type and what can be done to prevent it from occurring. Even not knowing what one type of attack does can be dangerous since there will be no defense against it if it happens.

All of this is important to study because any form of spending involved from fighting against hackers has increased significantly as time progressed. Since the tech industry continues to grow with no signs of slowing down, hackers will also grow in number. But hackers can be combated easily. With a proper, well-maintained defense, any hacker can be kept at bay indefinitely. However, not everyone is taking the steps necessary to ensure that this happens. If more awareness is brought to the issues at hand, then this research will have proven to be helpful. Hackers cannot be given the ability to terrorize the cyber world. As people rely on the cyber world more and more for our everyday lives, maintaining the safety of the internet is one of the most important things people can do.

Literature Review:

Technology has become a necessity in modern life, whether we want to admit it or not. While the reception of technology has been mostly positive, not everyone agrees that it has been completely beneficial to society. Technology has brought society a lot of advancements in the modern age. It is now much easier to keep in contact with others on a more reliable basis, as mailing letters to people is now nowhere as reliable as calling them, emailing them, or messaging them on social media sites like Facebook or Twitter. Unfortunately, having this type of technology can be harmful to children, as they can soon become enraptured in their screens for several hours a day (White, 2016). Having all this technology could certainly inspire more children to enter the computer science field when they become older, but they must be taught how to handle their technology properly. If these children are not taught the importance of limiting their technology usage, they can potentially become obsessed over it. This has the risk of causing the child to take an interest in hacking, and someone that young should not be able to wield such power. These people, if not instructed properly, run the risk of becoming a black-hat hacker, which is a type of hacker that will not hesitate to break the law for selfish gain. Taylor claims that people hack for six reasons, and they are, "Feelings of addiction, urge of curiosity, boredom with the educational system, enjoyment of feelings or power, peer recognition, or political acts," (Taylor, 1999). However, as the number of hackers continues to grow, the countermeasures for dealing with these hackers do not increase at the same rate. When more forms of technology are released to the public, it may increase the number of hackers as well because they will either want to learn more about the new technology for studying purposes or they will exploit the new system to gain leverage of some kind.

It may be nice to build technology that will assist people in the long term, but if a defense cannot be built, then there really is no point in building said technology in the first place. In order for a large tech company to be able to lead by example, they must be able to not only create revolutionary technology, but they will need to take the necessary steps to make sure that all of the work that went in is not wasted. Unfortunately, it does not seem that these companies are taking the necessary precautions to protect themselves. A study conducted by Big Brother Watch showed that in the U.K. alone, about 37 cyber-attacks can occur in the span of just one minute (Ashford, 2018). That is way too many attacks for a country to handle if they are coming in that fast. That means that millions of these attacks can happen in one year, or maybe even more. In order to combat these newfound threats, cyber security must be prioritized over anything else. However, some studies have found that cyber security does not get prioritized, but why does that happen? A study involving 1,300 IT professionals was conducted only 66% of them viewed cyber security as a priority, with 30% of the 1,300 saying that they had a plan to counteract attacks and only 19% of those believing that a cyber-attack could be stopped by their organization if one of these were to occur. Companies know a lot about cyber security, but they fail to combat it because they "neither have the confidence nor the plans to tackle the problem," (Glick, 2018). In order to handle a massive problem like this, some solutions need to be figured out. Even though not everyone is willing to come up with solutions, a few people have stepped in to contribute a possible answer. On the other hand, Kennedy provides a solution suggesting "constant and timely updates to security software as well as network and application software both for business and personal devices," (Kennedy, 2017). The solutions are out there for people to figure out, but the initiative needs to be found first in order to establish a proper starting point. But once a starting point is found, and then any cyber-attack can be eliminated if it is handled correctly.

Currently, the Internet is one of the most powerful things in the world. Nearly every country in the world has some type of internet presence, but some countries can obtain influence on the internet easier than others. One of the countries that obtained power over the internet incredibly fast was China. Currently, China is known for having one of the fastest growing economies in the world. Beginning after 1978, China underwent a rapid rate of economic growth that continues today. The leader of China at the time, Deng Xiaoping, introduced numerous reforms to agriculture, science, industry, and the military. This would later be known as the Four Modernizations, and these policy changes greatly bolstered China's economy. China was able to grow at a very rapid rate once the Four Modernizations were implemented, and they quickly became a superpower in the world. Even though China was behind prior to 1978, they were able to modernize quickly and develop many forms of infrastructure such as new roads that allowed them to compete with other countries on the global scale. Once the Internet began to spread across the world, China viewed it in a different manner compared to other countries. China appeared to treat the Internet as a new form of media since radio programs and television shows were placing their recordings on the Internet for others to view whenever they wanted (Lin, 2019). Out of all the countries in the world, China has the most hackers in the world. While this may be because China has one of the highest populations in the world, China's rapid growth has encouraged numerous Chinese people to gain knowledge about how to use computers. Those people who can get good knowledge on how to use computers will be able to learn how to use them in more advanced methods, such as hacking.

China was able to gain a lot of influence in the world very quickly. By 1999, during the Kosovo War, China had been able to breach NATO's website. They were able to do this via a malware attack and used this opportunity to explain that they did not want Kosovo to be bombed (Lin, 2019). Since the Internet was still very young, cyber-attacks were not advanced at all. Most of them involved tampering with websites, like China's NATO attack. After the United States attacked China's interests in Yugoslavia, the two countries began performing cyber-attacks against each other. Since the Internet was more primitive back then compared to now, the only attacks that could be carried out involved tampering with website pages in order to spread false information or propaganda (Lin, 2019). China quickly learned that the Internet is something that they could use to acquire more power, so they sought to learn how to control it to suit their narratives. By 2005, China had greatly mobilized its cyber force and were using it to spread their influence over the world. They developed a type of attack known as the APT, or advanced persistent threat, where they used psychological warfare to befriend a potential victim, wait until said victim gives them access to their computer, then betray them and take over their computer (Lin, 2019). However, an attack of this magnitude has a large list of demands that cannot be done by any ordinary hacker. This is because APT attacks are a type of espionage and are usually only carried out by governments or some sort of influential rich person. APT attacks require a lot of time, money, and resources, and can thus only be handled by the best of the best. Despite the type of hacker that must carry out an attack of this caliber, anyone is capable of being targeted by an APT attack. The U.S. government had caught onto this by 2006, and they were certain that an attack of this kind could not be defeated by a simple anti-virus (Lin, 2019). After seeing how successful these APT attacks were on their targets, China became more aggressive with them. The Chinese quickly began attempting to gain the trust of people who were deemed vulnerable or those who had a lot of power, and after gaining that trust, they would figure out how to take over that person's computer. The most common way the Chinese were able to succeed at this was to trick their intended target to open a file. This file was generally something unassuming, like a Word or Excel document. (Lin, 2019). However, these files were filled with malware that would spread across their computer quickly. After opening the document, the host's computer would become infected, and the Chinese gained control over it. These people likely opened the document because they had believed that the file did not contain anything valuable and that their friend was just trying to share some interesting information. But before long, the host would learn that their "friend" was nothing more than a hacker trying to sell valuable personal information for money or power.

In the present time, China has changed its tactics. While its APT attacks have almost completely stopped, China has shifted towards a policy of censoring other countries in the hopes of keeping the propaganda going. China has wanted to stop the influence of non-Chinese media across the country for similar reasons, so they have taken the steps to ban some forms of social media and some websites, such as Facebook, YouTube, and Google (Lin, 2019). China has effectively gained control over what happens on the Internet inside of China, but some of the Chinese people who are unsatisfied with how China is running the country have attempted to circumvent this. China is known for censoring anyone who dares to challenge their authority, by removing negative comments said about them or attempting to arrest those who challenge China otherwise. These changes have caused China to develop their own cyber security in order to control their narrative. China has its own firewall system separate from the rest of the world in order to control what enters their networks. China has emerged as one of the biggest threats to cyber security due to its separate network.

There are many other types of cyber-attacks, and it is important to have a strong understanding of as many of them as possible. Sometimes, hackers will find a way to breach another person's computer. They can do this with phishing scams. Phishing scams are where a person will receive an email from someone else saying to click on a link or download a file, and if they do it, then their computer will be infected with malware that will completely take over their computer. That type of attack can be done to large companies, too. If even one employee falls for this type of scheme, then whoever took over the employee's computer can breach important company files and steal important information. An even worse scenario to come from this may be if that computer that was breached gets the ability to spread the malware even further by infecting other computers in a similar way. Since the other company employees think they're getting an email from an employee about work, they may open the email and get their own computer infected, too. With every computer in the network having been taken over by malware, millions of dollars can be lost.

Cyber-attacks are also present in the world of cryptocurrency. Most cryptocurrency exchanges are done on a blockchain, where transactions can be conducted in concise manners quickly. 51% of attacks occur when over half of the network of a company is taken over by hackers. In the world of cryptocurrency, 51% attacks function a little bit differently. There, 51% of attacks are done to take over more than half of a blockchain, thus allowing hackers to have control over it (Sayeed and Marco-Gisbert, 2019). Some people like to keep their bitcoins in what's known as a hot wallet. Hot wallets are a type of software where digital money such as bitcoin can be stored. Since they are connected to the internet, they are vulnerable to cyber-attacks. A 51% attack can do millions of dollars of losses to bitcoin companies such as BitCoin Gold and Verge (Sayeed and Marco-Gisbert, 2019). This type of attack primarily targets hot wallets, with hackers hoping to run off with as many bitcoins as they can grab. Another dangerous type of cyber-attack is the destructive denial of service attack or DDoS. With this type of attack, hackers can stop activity completely on certain networks, which is another very damaging and costly attack on companies. In addition to completely stopping activity on the network, it has another major repercussion in the world of cryptocurrency. DDoS attacks can halt transactions on a blockchain while allowing illegal transactions done by the hackers to bypass the system (Sayeed and Marco-Gisbert, 2019). In a severe situation, attackers can perform a permanent denial of service attack, where the network gets taken down forever and the original company must replace everything themselves (Pool, 2013).

Cyber criminals have been getting smarter when it comes to cyber-attacks. Attackers have developed new forms of cyber-attacks whereas cyber security professionals must adapt and keep up to these new assaults. One example of a cyber-attack that hackers have come up with to combat the growth of the cyber security field is the use of ransomware. These criminals have managed to develop a special type of ransomware that is able to function while it is not online. Under regular circumstances, ransomware like this would be stopped by a firewall (Anderson, 2017). If these professionals were not able to completely stop the attack, they were at least able to keep the damage at a minimum (Anderson, 2017). In order to combat these attacks, professionals must learn new tactics and methods of suppression. When combating a cyber-attack, the primary method of dealing with it is known as risk mitigation. Risk mitigation is a set of processes that professionals go through to stop these breaches. These processes can prevent, hold, and suppress cyber-attacks (Anderson, 2017). In addition to risk mitigation, another process like it called risk agility is designed to help make these cyber-attacks noticeable faster. In addition to helping make these attacks seen more quickly, risk agility also assists in the foundation of team building, since cyber-attacks typically require a group of people to suppress sufficiently (Anderson, 2017). Another excellent method for handling the aftermath of a cyber-attack is checklists. Checklists are generally used for procedures that have many steps and for procedures that cannot function successfully if one step is left out or incomplete. These checklists are handled by a group known as the Team Resource Management, or TRM. (Anderson, 2017). The TRM ensures that everyone in the group is able to combat a cyber-attack properly while also making sure that everyone involved is able to react quickly to make sure that the attack does not spread and cause significant amounts of damage.

Combating cyber warfare is a big challenge, but it can be done with the right resources, knowledge, and people for the job. While not necessarily the best solution, countries have planned a treaty that might alleviate some issues. In 2010, several countries gave out ideas for creating a worldwide treaty for handling cyber threats. These countries suggested that the United States, Russia, and China each release information on how they would handle cyber-attacks in the future. Since the U.S., Russia, and China were the three most powerful countries at the time, having these three countries agree on this would be great for ensuring that the cyber space was safe (Pool, 2013). The United Nations has also been tasked with handling cyber-crime, and numerous suggestions have been pitched to them. The U.N. has a pair of divisions known as the Commission on Crime Prevention and Criminal Justice and the Office of Drug Control and Crime Prevention. The Commission on Crime Prevention and Criminal Justice is tasked with coming up with a plan to prevent and control cyber-crimes. The Office of Drug Control and Crime Prevention is tasked with putting that plan into action (Pausto, 2004). With these divisions tasked with handling cyber-crime, the United Nations has been providing as much assistance as possible on tackling the issues.

One of the biggest threats to cyber security is vulnerabilities. A vulnerability is something that is flawed in a network system and can be exploited by a cyber-criminal for their own personal gain (Dunn Cavelty, 2014). An attacker who is successfully able to exploit the vulnerability can breach into and potentially take down a network. Vulnerabilities like these can be especially exploitative when dealing with zero-day attacks. Zero-day attacks are much more dangerous than other attacks since they involve zero-day vulnerabilities or issues in a network or computer that are either unknown or have failed to be addressed. However, not every zero-day vulnerability is found for good reasons. Even the United States government has utilized these zero-day vulnerabilities to attack other countries. The NSA has found some of these zero-day vulnerabilities to attack certain strategic points of the Internet. When this information was released to the world, some programmers intentionally developed some zero-day vulnerabilities in the hopes to sell them to the government to a profit for money (Dunn Cavelty, 2014). Actual zero-day vulnerabilities are much harder to find since not everyone is being honest about reporting them to the rest of the world due to their own selfish wants and desires. With the prospect of making a lot of money quickly clouding the judgments of top programmers, finding integrity in the industry has become a challenge that must be surmounted.

When combating cyber-crime, it is important to understand who potential victims of a cyber-attack can be and why it is difficult to track down their attackers. While anyone is technically able to be a victim of a cyber-attack, there are some people who are much more vulnerable than others. For example, in the past, an elderly person was very vulnerable to having their personal information stolen by someone who wanted to get a lot of money. While this situation does not necessarily involve hacking, there are other situations where an elderly person can be a victim. It’s believed that the people who are the most likely to be victims are teenagers and the elderly since both the youth and the elderly are the ones who are the least aware that these attackers exist (Li, 2018). Once a computer becomes infected, it can remain infected for long periods of time, often weeks or even months. That is why it is important to ensure that all computers receive proper updates, defrags, and maintenance checks. A person who has been victimized by a cyber-criminal may not notice that they have been hacked for months, and by the time they do notice, it is likely that the criminal developed some sort of loophole to ensure they continue having control over the computer (Li, 2018). Sometimes, attackers may not necessarily go after the actual property of a victim, and instead try to damage their state of mind. Some attackers have a mindset of wanting to cause some damage to the victim’s mental health rather than their wallet. Those types of attackers may find a twisted feeling of joy when they learn that the person that they stole from is not able to make a mortgage payment, pay off a credit card loan in time, or do their taxes in time. A cyber-criminal may still find psychological enjoyment out of torturing someone else, even if they are unable to make any money from them (Li, 2018). Figuring out the identity of an attacker is not easy, though. The Internet allows people to surf the web anonymously, which makes it very difficult to figure out the identity of a person who committed a cyber-crime. Cyber-criminals on the Internet can fabricate their identities on forms that ask for an email address, a physical address, or a name (Li, 2018).

Regular people are fully capable of doing their own part in combating cyber-crime, too. Those who desire to keep their computers safe can protect it the best way possible with multiple different methods. Some of the main methods a person can use to keep their computer protected include firewalls, authentication, and encryption. If a cyber-attack can get through the firewall, users can detect and isolate the attack to keep the damage at a minimum. (Nong Ye et al., 2001). Once a cyber-attack is detected, the computer can potentially boot out an attacker if one is detected. In addition to keeping their computers up to date, people can take other precautions to avoid becoming a victim of a cyber-attack.

Research Question:

The purpose of this research is to understand why cyber-attacks are not handled properly in modern society, and what people can do to learn from our past mistakes when battling cybercrime. By 2021, the world is expected to spend over $1 trillion on cyber security and $6 trillion on cybercrime. People cannot afford to continue overlooking cyber security, as it will soon become too big to fight back against. Different types of impactful cyber-attacks that have occurred and their resulting effects have been explained, and their significance have been elaborated upon. From there, ways to combat cyber-attacks and the growth of cybercrime will be explained with the end goal of educating more people about why it is important to keep computers secure since cybercrime will continue to rise at a very rapid rate. With all of this knowledge in mind, educating more people about the importance of cyber security and how countries have battled it is another reason behind this research.

Methodology:

Information has been gathered for this study in two different ways. Firstly, research that has already been done has been used to support the argument proposed. Since the industry is growing at a quick rate, new information is constantly being brought to light. For the purposes of this study, research from over 20 years ago will be excluded, as these sources may be outdated now and that could weaken the argument the thesis is presenting. A wide scope of the range has been dedicated to learning more about the industries that have to work with cyber security. Deep down, every major company that exists nowadays, regardless if it is a tech company or not, still must place some effort into cyber security's influence on their company. The scope of this study was not just limited to the United States and how their version of the Internet has grown. Some investigation has been done into how other countries handle their usage of the Internet as well, such as China. Research has been done on some influential types of cyber-attacks, the amount of damage they are potentially able to cause, and the lasting repercussions of them. Some research was centralized on ways we as people can combat these cyber-attacks. Even if the answer to this question is simply being more alert to our computers, studies can be done to help elaborate on why that is so important. Research has also been dedicated to the world of cryptocurrency and how that side of the Internet has been affected by cyber-attacks. Since the cryptocurrency industry is worth millions, even billions of dollars, this is a very profitable market for cyber-criminals to breach into. Since bitcoins were worth up to $20,000 at one point, there is a very strong market for cybercrime there, even in the present day where it is not worth as much but still very valuable, nonetheless. The bulk of the study has been spent on the research and the studies, but another method has been performed, and it involved individual research that has been used to strengthen the purpose of the study even further.

Secondly, a hack lab was built to work on some self-driven experiments. How the lab works is complicated, but with enough diligence, it can be learned. The lab can run several different programs such as Kali Linux, Metasploit, and Cyborg Hawk, all of which can be used for hacking purposes. However, the lab cannot function by itself; there needs to be something to hack. Thankfully, all the materials that are needed for this have been obtained before beginning the study. Several old phones have been collecting dust back home and all of them still work. So, for this experiment, the goal is to see if hacking into these phones is possible to do within a time frame of one month with no prior experience. The intent of this was to see how encrypted everything inside is, while the time frame aspect is to see if learning how to hack within a short period of time is possible. The issue here was that with a limited knowledge of hacking, it may be difficult to proceed. Despite that setback, that is the premise of the experiment. However, there is a possibility that this experiment will not be successful. If the experiment is ultimately not successful, the issues and difficulties will be discussed instead and how amateurs could learn from the mistakes made here. It is interesting to note that not everyone who hacks is experienced either. In 2015, a study was done showing that over half of the cyber cases that were looked at only succeeded partially due to the abilities of the attacker. Instead, these other attacks only succeeded due to mistakes by the company that the attacker was trying to infiltrate (Popescu and Popescu, 2018). From this, even though it will be difficult to hack into a phone with no prior experience, all the tools needed to do so are available. The legality of this is not an issue because this is an example of white-hat hacking. White-hat hacking is commonly utilized by professional penetration testers, as they are tasked with infiltrating a security system to find out vulnerabilities and then report them back to the company who hired them. After these vulnerabilities are found, these issues are reported to the company that hired the tester and they are tasked with fixing the issue to ensure a hacker is not able to break into the system.

Results and Discussion:

From all the research that was gathered and combined with the individual research that was done, it is safe to say that cyber-crime is still an issue that tends to be overlooked in the modern age, even though many should be aware of how dangerous it is. It is not possible at this point to simply abandon all the technology that has been developed since life without it would be substantially more challenging. Humans have come to view technology as an absolute necessity and removing it would not end the primary problem. If the world were to hypothetically make technology illegal, a repeat of what happened during Prohibition would likely take place. Technology would never go away; it would instead be moved “underground,” and people would continue to use it in secret.

Since there are many ways a cyber-attack can be performed, combating each type of attack requires a lot of knowledge and awareness about them. With many different types of cyber-attacks out there in the world, there are many ways to combat each one. However, the cyber-attacks themselves are not the only threat people must face. There are many countries out there in the world such as China and Russia who want to use their Internet influence to cause divisions between other countries.

From the original research that was conducted, building a hack lab was not particularly complicated, but performing the actual hack itself proved to have a rather steep learning curve towards newcomers. To build the hack lab, a few supplies were needed. For the hack lab to be fully functional, a working computer is needed, and some software programs will need to be installed on said computer. Oracle VirtualBox is the best way to utilize the different types of hacking software. After installing Oracle VirtualBox, it is possible to add new virtual machines into the system. Systems such as Metasploit and Kali Linux were used during the experiment to see if it would be possible for a person to learn how to hack in a short period of time. Metasploit is a software that assists in figuring out vulnerabilities, whereas Kali Linux is a software that is specifically designed for ethical hacking and penetration testing. Finally, something to break into for experimental purposes was needed as well. For this experiment, an old cell phone was utilized. Finally, having strong knowledge of the Command Line is strongly recommended. Command Line is a programming language where the user inputs a command for the computer's operating system to perform. For example, inputting -h into the program allows the user to learn a list of other commands that they can input. It is possible to use Command Line to access certain folders and files on a user's computer and make changes to them accordingly. Despite successfully obtaining all the necessary supplies, it was not possible to hack into the intended phone within the timeframe provided. The learning curve of using these programs and programming languages could not be surmounted during the timeframe of this experiment, but a lot was still learned.

For this experiment, the plan was to create what is known as a payload. A payload is a file that can be used to retrieve the personal information of the user of the phone. Using this would essentially create a smaller version of a phishing scheme, where this payload would be sent off in an email to the person who used that phone. If the link were to be clicked on, the payload would be able to gather the personal information of the user and send it back. However, performing this experiment within the given time frame proved to be a challenge that could not be overcome.

From all of this, it can be concluded that hacking requires a lot of time and effort to learn, much more so than what was experimented upon. Those who become serious full-fledged hackers give themselves a lot of time and training into making sure their attacks are carried out properly. Those who have become full-fledged hackers tend to start very young, likely when they are only just becoming teenagers, and they quickly develop an interest in computers. However, many who begin to develop start to go overboard and try to gain as much power or money as they can. In order for them to successfully reform, the only real solution has been to give these hackers jail time and rehabilitate them by taking their computers away from them. While this has not proved to be completely successful, it has been able to transform many black-hat hackers into white-hat hackers.

Just having only one month to complete the experiment proved to be a poor move in the planning process due to the amount of time needed to learn how to hack the phone. There are some better ways to go about this experiment now that it has been concluded, such as increasing the time frame or providing a period of time dedicated to understanding the material first before commencing the experiment.

For this experiment to have a greater chance of success, the amount of time to execute it should be increased, from one month to maybe three months. With the amount of time that was set aside for this project, completing it may have seemed feasible during the planning stages, but was not successful when following through with it. The experiment's end results could be repeated if not enough time is given to remaking it. The primary misstep that was made was not having the best understanding of Command Line, despite spending a long time trying to study it and learn how it operates. Even so, with the limited time frame combined with the lack of knowledge going in, the experiment still managed to help spread awareness about the importance of having cyber security in a world that uses technology to make day-to-day tasks much more simplified. Coming out of the experiment, those who wish to attempt to remake this experiment might want to either gain the knowledge before beginning the experiment or instead give themselves more time to get the task done. As a possible alternate way to go about this experiment, those who want to replicate it should give themselves one month to learn the basics of Command Line and the world of Oracle VirtualBox. After that month passes, those would get another month to attempt to breach the security of a phone. If either more time to perform the experiment is given or if some separate time is provided to give the researcher a chance to learn the fundamentals is given, then it is much more likely that they would be able to provide a much more favorable outcome to this experiment.

Conclusions:

The world of cyber security is massive, and it will continue to grow without ever stopping. With all of this information in mind, combating the growth of cybercrime will be a large challenge that will require as many competent programmers as possible. Since there are several countries in the world that have plenty of power and influence in the cyberworld, staying up to date on current cybercrimes and being proactive in learning about as many types of cyber-attacks as possible is a good way to remain prepared in case one strikes. There are plenty of ways that cyber security can be combated and those who know how to deal with each attack can stop or suppress it. Even if an attack is not fully stopped and only suppressed, the amount of damage that is done will be significantly reduced and the cost of repairs will not be as significant as it could have been.

Looking towards the future, those who want to take part in a similar experiment should be able to set aside plenty of time for their own project so as to not replicate the mistakes that were done during this project. Ensuring that all the necessary supplies are in order combined with providing enough time to learn how to code in Command Line and knowing where to go should an error occur. Perhaps other virtual machines could be utilized in addition to the ones that were used throughout this experiment. Regardless, if the experiment was planned out a bit more carefully, a successful result could have happened. Even though it did not, a lot of knowledge was still gained while carrying it out. Even though this particular experiment did not yield a positive result, it is entirely possible for another person to replicate something like this and be more likely to find success.

References:

Anderson, Kerry. “Using Agility to Combat Cyber Attacks.” *Journal of Business Continuity & Emergency Planning*, vol. 10, no. 4, Summer 2017, pp. 298–307. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=buh&AN=123709303&site=eds-live&scope=site.

Ashford, Warwick. “Many UK Local Councils Fail to Report Data Breaches as Cyber Attack Pressure Grows.” Computer Weekly, Feb. 2018, pp. 4–6. EBSCOhost, rlib.pace.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=128220780&site=eds-live&scope=site.

Dunn Cavelty, Myriam. “Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities.” *Science & Engineering Ethics*, vol. 20, no. 3, Sept. 2014, pp. 701–715. *EBSCOhost*, doi:10.1007/s11948-014-9551-y.

Glick, Brian. “Reality of Cyber Attacks Must Focus Minds.” Computer Weekly, Feb. 2018, p. 14. EBSCOhost, rlib.pace.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=128220783&site=eds-live&scope=site.

Kennedy, Mike. ‘Equifax hack shows we need more regulation.’ *Daily Herald* [Arlington Heights, IL], 11 Oct. 2017. Infotrac Newsstand, http://link.galegroup.com.rlib.pace.edu/apps/doc/A509048277/STND?u=nysl_me_pace&sid=STND&xid=821e13aa.

Kuru, Huseyin. “Evolution of War and Cyber Attacks in the Concept of Conventional Warfare.” Journal of Learning and Teaching in Digital Age, Vol 3, Iss 1, Pp 12-20 (2018), no. 1, 2018, p. 12. EBSCOhost, rlib.pace.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsdoj&AN=edsdoj.4620b940b3af42d6ba7dbe1371161f8e&site=eds-live&scope=site.

Nong Ye, et al. “A Process Control Approach to Cyber Attack Detection.” *Communications of the ACM*, vol. 44, no. 8, Aug. 2001, pp. 76–82. *EBSCOhost*, doi:10.1145/381641.381662.

Pocar, Fausto. “New Challenges for International Rules against Cyber-Crime.” *European Journal on Criminal Policy & Research*, vol. 10, no. 1, Mar. 2004, pp. 27–37. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=sih&AN=17620601&site=eds-live&scope=site.

Pool, Phillip. “War of the Cyber World: The Law of Cyber Warfare.” *International Lawyer*, vol. 47, no. 2, Fall 2013, p. 299. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=edb&AN=95779529&site=eds-live&scope=site.

Popescu, Gheorghe N. and Popescu, Cristina Raluca Gh. “Risks of Cyber Attacks on Financial

Audit Activity." Audit Financiar, Vol 16, Iss 149, Pp 140-147 (2018), no. 149, 2018, p. 140. EBSCOhost, doi:10.20869/AUDITF/2018/149/140.

Sarwar Sayeed, and Hector Marco-Gisbert. "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack." *Applied Sciences*, no. 9, 2019, p. 1788. *EBSCOhost*, doi:10.3390/app9091788.

Taylor, Paul A. "Chapter 3: The Motivations of Hackers." *Hackers*, Taylor & Francis Ltd / Books, 1999, pp. 45–66. *EBSCOhost*, rlib.pace.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=sih&AN=18059913&site=eds-live&scope=site.

White, Jorgia. "Screen Time Harsh Reality; The Negative Effects of Technology." *Coolum &* North Shore News (Coolum Beach, Australia), 2016. EBSCOhost, rlib.pace.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsgin&AN=edsgcl.467751982&site=eds-live&scope=site.

Xingan Li. "Crucial Elements in Law Enforcement against Cybercrime." *International Journal of Information Security Science*, vol. 7, no. 3, Sept. 2018, pp. 140–158. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=aph&AN=133550408&site=eds-live&scope=site.

Ying-Yu Lin. “China Cyber Warfare and Cyber Force.” *Tamkang Journal of International Affairs*, vol. 22, no. 3, Jan. 2019, pp. 119–161. *EBSCOhost*, doi:10.6185/TJIA.V.201901_22(3).0003.