# The Rapid Increase of Ransomware Attacks Over the 21st Century and Mitigation Strategies to Prevent Them from Arising

Sanjay Jacob

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2023

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial
fulfillment of the requirements for graduation from the
Honors Program of Liberty University.

_____
Mike Kiperos, D.B.A.
Thesis Chair

_____
James McNicholas, Ph.D.
Committee Member

_____
James H. Nutter, D.A.
Honors Director

_____
Date

## Table of Contents

## Abstract

Cyber-attacks have continued to become more common throughout the past century as more people are exposed to the Internet. Every year, various studies, reports, and scholarly research is done to emphasis the rapid increase of attacks. In this honors thesis, the student sought to gather further information about the rise of ransomware attacks, various cyber threats, discuss the psychological manipulation that exist, and provided the reader with an ethical complement of cyber-attacks. Additionally, case studies from previous research have been analyzed and mitigation strategies have been explained to provide the reader with practical application. This research emphasizes in on key issues that relate to the most recent cyber-attacks and the effects that it has had on the world.

# The Rapid Increase of Ransomware Attacks Over the 21st Century and Mitigation Strategies to Prevent Them from Arising

Throughout the 21st century, there has been a continued increase in technology use, which significantly influences people worldwide. As the world continues to develop, technology is becoming more advanced, making itself commonplace. However, while the growth of technology has been beneficial in certain areas, there is a greater chance becoming a cyber-attack victim. Reports have shown that 85% of organizations were attacked at least once in the past 12 months, which is up from 9% from 2023 (Ramel, 2023). Throughout this century, and particularly in this past decade, many businesses and companies have been victim of cyber-attacks, particularly ransomware attacks. For example, an event like the WannaCry Ransomware Attack was unprecedented in scale, impacting over 250,000 computers in over 150 countries in a few days (Trautman & Ormerod, 2019). By analyzing various incidents like the Colonial Pipeline, WannaCry, and Kaseya, Ransomware Attacks, companies can be better prepared to secure their infrastructure. Throughout this paper, these three ransomware attacks will be analyzed as a case study, where the causes and effects will be discussed in depth. Ransomware attacks and vulnerabilities can be mitigated with proper prevention and protocols. However, as the use of technology continues to grow, businesses and individuals must be able to understand how to protect themselves from the various security vulnerabilities that exist. Analyzing the rapid increase of ransomware attacks and providing mitigation strategies can serve as a tool for businesses and originations in hopes of lessening the potential attacks that could occur.

## What is Ransomware?

Ransomware is a type of malware that encrypts a file, making it completely unusable. It is appropriately defined as “malicious software designed to block access to applications or files on a computer system until a sum of money is paid” (Andrew Sears, 2021, p. 2). Typically, malicious attackers demand a specific amount of money to decrypt the files on the victim's system. Unfortunately, this attack is common, and attackers continue to compromise systems. Ransomware attacks increased drastically in 2022, being involved in 25% of all breaches (Kerner, 2023). As more people continue to use the Internet and the reliance on cloud-based software grows, ransomware is an unfortunate likelihood that can infiltrate and compromise sensitive data and critical assets. Ransomware must be addressed, and mitigation strategies must be implemented to reduce these issues. Furthermore, to defend against the ransomware attacks, a vigilant security posture is vital (Yuryna Connolly et al., 2020). By having a security posture in which there are careful observations of potential threats, a business can defend itself against ransomware attacks.

The three primary forms of ransomware are “locker, crypto, and scareware” (Beaman et al., 2021, p. 2). Regarding locker ransomware, user access can be limited, and the files may be locked. In addition, it can encrypt specific files that can lock the computer screen and keyboard. However, it is generally easy to resolve by rebooting the computer in safe mode or running an on-demand virus scanner (Beaman et al., 2021). Regarding scareware, it uses various manipulation tactics to block essential computer functions, leaving minimal to no harm (Beaman et al., 2021). For example, they may use pop-up ads to manipulate users into assuming that they are required to download specific software, thereby using coercion techniques for downloading malware (Beaman et al., 2021). Rather than lock the device or encrypt any data, the attackers

employ fear to exploit their victims (Andronio et al., 2015). Crypto ransomware differs in that the computer's primary function is not interrupted, but the sensitive files on the computer are encrypted. Unlike locker ransomware, crypto ransomware is often irreversible as current encryption techniques (e.g., A.E.S. and R.S.A.) are nearly impossible to revert if appropriately implemented (Beaman et al., 2021). While these three primary forms have their differences and similarities, these attacks can leave lasting damage, and businesses must prioritize implementing and providing updated security policies and procedures.

Ransomware attacks can negatively impact businesses and organizations, significantly harming a company. It can reduce the productivity of a business, lead to a significant loss of finances, and negatively interfere with a business's day-to-day operations (Beaman et al., 2021). As ransomware attacks continue to rise, the negative impacts continue to be more present throughout businesses. The global survey "The State of Ransomware 2021" survey showed that among over 2000 respondents who claimed that their organizations had fallen victim to a ransomware attack, the average total cost to an organization to rectify the impacts of a ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid) was $1.85 million USD, which is more than double the number from 2020 (Beaman et al., 2021). Unfortunately, since the attacks can result in a business or organization losing its data permanently, a decision must be made on whether to pay the ransom. The decision to pay the ransom is a decision to be made by the business, and they must prepare for it in advance, having a clear understanding that they might not retrieve their information back completely (Hofmann, 2020). Throughout this decision-making process, the affected companies must come together and understand negotiation techniques as well as the potential risks that exist. Since the pandemic, ransomware attacks have increased, negatively impacting businesses

and organizations. In addition, the attackers have preyed on the weak by attacking hospitals, vaccine research labs, and contact tracing apps (Pranggono & Arabo, 2020). Understanding the adverse effects that ransomware is having on various companies should encourage businesses and organizations to implement more robust security measures to mitigate future attacks.

## How Cyber-Attacks are Perpetrated

As previously explained, the rapid growth of technology has led to cyber-attacks becoming more common throughout businesses and those exposed to the Internet. Unfortunately, much of the reasoning behind these cyber-attacks is either politically or criminally motivated. Understanding the nature of such a cyber-harm is critical to ensure that the controls and methods of mitigation that companies deploy will be proportionate to the risks and effective (Agrafiotis et al., 2018). A better understanding of how cybercriminals perpetrate attacks can improve the security controls of a business and their methods to mitigate future attacks. Throughout security awareness training, the goal should be to move employees toward intrinsic motivation, where they see the value of security, develop a curiosity for learning, a desire to make ethical decisions, and feel a sense of ownership and empowerment, leading to them practice good behaviors (Haney & Lutters, 2020). Having employees who understand the importance of security can help them make more thorough and informed decisions and benefit the organization as a whole. Using technology throughout a business is imperative for its survival, and if properly secured, the chances of being attacked can be reduced.

From phishing attacks to SQL injection to ransomware attacks, these cyber-attacks can be carried out through various methods. These methods can have various effects on a business and the people who work throughout the organization. With attacks like ransomware and others,

cybercriminals usually perform this and make it their goal to take advantage of those around them. Cybercriminals usually exploit users with a lack of digital/cyber ethics or who are poorly trained in addition to technical vulnerabilities to reach their goals (Alkhalil et al., 2021). The psychological manipulation that attackers perform on their victims can be intense and cause significant damage to an organization or business. Unfortunately, the root of this psychological manipulation is tied to the pursuit of financial gain for the attacker to reach a specific goal. The goal for the attacker would be to carry out the attack. Often, these cyber-attacks are prepared to target either financial or social gain (Arachchilage & Love, 2014). The individuals who perpetrate cyber-attacks frame a mindset in which they desire to attack and exploit innocent individuals to fulfill their corrupt desires.

Attackers perform psychological manipulation toward victims throughout these attacks, which has caused much damage. Psychological manipulation in this sense relates to the act of social engineering. Social engineering can be defined as “the act of manipulating human beings, most often with the use of psychological persuasion, to gain access to systems containing data, documents, and information that the social engineer should not have access to obtain” (Washo, 2021, p. 1). An attacker’s primary goal is to undermine their victim's resilience by instilling a sense of fear and vulnerability that erodes confidence in the ability of the government and law enforcement agencies to protect citizens against future attacks (Gross et al., 2017). Understanding the psychological manipulation behind the attacks allows businesses and organizations to understand why specific attacks occur. This further understanding of psychological manipulation allows decision-makers to create and develop strong policies. By enforcing strong network security policies, the business would have a higher success of mitigating attacks from occurring in the future. Rather than a kinetic force, cyberterrorism

employs malicious computer technology and aims to further political, religious, or ideological goals by harming civilians physically or psychologically (Gross et al., 2017). Even though the organization can be harmed through a cyber-attack, the people who work there can also be harmed. An attacker's malicious intent can lead those who work in the organization to be taken advantage of. Throughout a study on threat perception, exposure to past cyberattacks and exposure to simulated cyberattacks increased perceptions of threat (Gross et al., 2017). While threats and malicious intentions will continue to grow, if an organization takes the proper steps to secure its infrastructure, it can lessen and help mitigate future attacks.

## Case Studies of Ransomware Attacks

As society continues to evolve, technology is becoming more present throughout our lives and ransomware attacks are continuing to grow. Studies show that ransomware has grown a lot over the years, costing the world $20 billion in 2021, and expected to rise to $265 billion by the year of 2031 (Brooks, 2022). From the Colonial Pipeline, to WannaCry, to Kaseya ransomware attacks, these are just a few examples of attacks which have wreaked havoc on millions of people throughout the world. As explained, attacks like these three have led to billions of dollars and resources to become depleted. The effects of this attack reinforce the critical need for improved security controls and protocols implemented throughout businesses. Organizations must have a clear understanding of the threats at hand and implementing strong security protocols to protect themselves and their data from being attacked or ransomed.

### Case Study: Colonial Pipeline Ransomware Attack

On May 7, 2021, Colonial Pipeline became a target by hackers who attacked the company, forcing them to shut down a major pipeline that carried various fuel types. The

hacking group, DarkSide, infiltrated their systems, which imposed them to shut down their pipeline, resulting in millions of people experiencing fuel shortages (Stephens, 2021). Additionally, the reports said that DarkSide stole over 100 gigabytes of data, leading to Colonial paying five million dollars in ransom not to have their data leaked (Stephens, 2021). Even though Colonial took care of the situation as quickly as possible, its effects on America showed the critical need to implement cyber security measures. As a result of these shortages, Americans started hoarding gasoline and waiting for hours to take preemptive steps to combat the lack of fuel (Voas et al., 2021). This attack showed the crucial need for companies to take preventative security steps to minimize these attacks.

The Colonial Pipeline System is critical for the fuel movement, and the shutdown of the pipeline made things increasingly difficult for consumers living in the middle of a pandemic. The system can move over 2.7 million barrels a day of fuel and supply eastern states with much of their fuel needs (Medlock III, 2021). As a result of the attack, it led to significant fuel supply disruption in Eastern states, particularly in the South. As stated previously, even though the system was restored and running back on May 15, the results of the attack led to a significant disturbance of fuel supply, heightened fuel prices, showing the critical need for security throughout every faucet of infrastructure (Stephens, 2021). The recent attack teaches the country and the world the importance of securing our systems, our energy infrastructure is vital for basic survival, and significant security enhancements must be made.

**Case Study: WannaCry Ransomware Attack**

In May of 2017, various organizations and businesses became targets by cybercriminals who infiltrated their devices that ran on an older version of Microsoft Windows Operating Systems. This ransomware attack encrypted the data on those systems and forced the victims to

pay a ransom to retrieve their data. From the loss of sensitive information to a disruption in regular operations and a significant number of financial losses, the effects of this attack were devasting (Sahi, 2017). One of the main reasons for this attack was the outdated software on the compromised computers. While Microsoft fixed the issue two months before the attack, those who did not update their systems were still susceptible to the attack. Hundreds of organizations running thousands of systems had failed to apply the patch in the first 59 days it had been released (Ehrenfeld, 2017). Due to this unpatched software, the Shadow Brokers, a hacking group, saw an opportunity in a flaw that they exploited by using a tool called EternalBlue. Unfortunately, this attack affected numerous United Kingdom National Health Service trusts, FedEx, Telefonica, Renault, and Nissan car manufacturing plants, U.S. universities, Russian governments, and Chinese A.T.M.s, among others, across 150 countries (Brewster, 2017). Making the necessary changes to safeguard their data is essential for businesses to implement because it can minimize threats and keep away cybercriminals.

The WannaCry ransomware attack highlights the critical need for increased security measures throughout businesses and organizations. Since ransomware is the most predominant cyber threat in the digital infrastructure, it is essential to understand how to minimize these security risks. Adhering to security policies and implementing security devices can help reduce these threats. This attack has made it clear the need for businesses, particularly in the health care industry, to step up efforts with cyber security so that organizations can implement every possible protection to defend against a future attack (Smart, 2018). In addition, this attack teaches the country and the world the importance of securing our systems, watching out for threats, and regularly scheduling maintenance and updates for devices.

## Case Study: Kayesa Ransomware Attack

In July of 2021, over one thousand companies and various organizations fell victim to REvil, a group of cybercriminals who infiltrated Kaseya's V.S.A. system, which allowed them to compromise customer devices and systems by injecting malicious software. This ransomware attack was sent out to the customers and their systems, which encrypted their data on those systems and forced the victims to pay a ransom to retrieve their data. As of July 23, 2021, Kaseya is the most significant ransomware attack by ransom demand at $70 million (Allen, 2022). Businesses and companies like Kaseya need to make the necessary changes to safeguard their data to keep away cybercriminals and lessen the looming threats.

The Kaseya Ransomware Attack highlights the dire need for businesses and organizations to implement increased security measures. Since ransomware is the most predominant cyber threat in the digital infrastructure, it is essential to understand how to minimize these security risks (Reshmi, 2021). Threats can be reduced by adhering to security policies and implementing the necessary patches and updates on security devices. The Kaseya Ransomware Attack has made clear the need for businesses, particularly those in the I.T. sector, to understand the dangers of ransomware attacks and to increase their efforts with cyber security to defend against future attacks. In addition, this attack teaches those in I.T. and those who are not to understand the critical need to secure systems, keep an eye out for threats, and regularly scheduled maintenance and updates for the software being used.

## Different Attack Vectors

An attack vector is a particular type of attack which can be exploited to hack into a system. Attack vectors use various resources to infect the computer and other networking devices

and ensures the passage to the intended target information (Tiwari & Dwivedi, 2016). There are many different attack vectors that exist. From phishing attacks to malware to social engineering, there are various attack vectors that exist. Attack vectors are dangerous methods that cyber criminals use to exploit various vulnerabilities and gain unauthorized access to various sensitive information. Regarding the three cyber-attacks that were analyzed in the case studies, attack vectors were used greatly. For example, in the Kaseya Ransomware Attack, malicious software was injected into the Managed service providers (MSPs) worldwide. It is evident in how there are various attack vectors that exist in ransomware that an organization must be aware of in order to protect their sensitive information.

One of the major attack vectors is malware, in which ransomware is a specific type of malware. Malware is the malicious software which can attack and compromise computers for users or the organization as a whole. The malware is programmed specifically to cause harm to computers and compromise sensitive information. Malware creators use a variety of techniques (polymorphic and metamorphic) in their code to make the malware look like it is a new version of an application or posed as item that a user can click on (Arunlal, 2019). As cybercriminals continue to get more creative with their attacking techniques and develop new methods, businesses and organizations must make sure to implement the proper security protocols to decrease the potential malware attacks that could exist.

Another attack vector that ransomware can be found on is through email attachments. Phishing attacks can take a variety of forms to target people and steal sensitive information from them, particular through using email (Alkhalil et al., 2021). In this attack, the attacker would hypothetically convince their victim to download or open a link that is disguised as a file that comes from a trusted sender. However, it is a malicious file that installs ransomware to their

computer system. This ransomware attack vector often takes the form of social engineering in which cyber criminals use deception to act as someone the recipient trusts and tricks them into giving them unauthorized access to corporate systems (Graham, 2022). This attack vector is particularly dangerous, as trust can be tainted, and businesses can have their sensitive data compromised through this.

While email attachments can transmit ransomware, there have been websites that pose to be genuine, but contain ransomware throughout the scripts. These seemingly legitimate or compromised websites are a perfect attack vector for cybercriminals because victims believe they are visiting a trusted site (Graham, 2022). This attack vector can lead to serious damage for a user or an organization, as the code could be automatically installed into the computer when the compromised site is visited. Once the ransomware is executed, it can infect the user's system and move laterally across the organization, encrypting files and data (Graham, 2022). Increasing cyber awareness and walking through potential cases like this with a business can help in reducing the number of attacks that could arise. It would be beneficial for an organization or business to make continued awareness of the potential risks that exist throughout the different attack vectors.

## Major Vulnerabilities

The vulnerabilities that can arise from the various attack vectors can decimate a system. Vulnerabilities can be found throughout software and hardware, and if not properly patched or fixed, they can lead to further complications. Unfortunately, with ransomware, it is the type of attack where it never fails to surprise in terms of its ability to identify vulnerabilities and loopholes in technology (Shah & Farik, 2017). There have been clear examples of vulnerabilities

in software and hardware that led to various ransomware attacks. There have been various vulnerabilities that have been exploited by attackers. From SharePoint vulnerability, CVE-2021-0604 to Microsoft Azure vulnerability, CVE-2021-38647, there are various vulnerabilities throughout software that exist and have been exposed ("Top Critical Vulnerabilities," 2022). Additionally, from the cases studied previously, it is evident how in the WannaCry Ransomware attack, the vulnerabilities that existed led to the severe ransomware attack which exposed various security threats, stole millions of dollars of assets, and decimated many people's lives.

As previously explained, ransomware attacks can infiltrate systems through vulnerabilities that are exposed. The SharePoint vulnerability, CVE-2021-0604 is a prime example of a vulnerability that exists throughout Microsoft SharePoint software. In this vulnerability, there is a remote code execution vulnerability in which the software fails to check the source markup of an application package ("Top Critical Vulnerabilities," 2022). Typically, throughout this type of vulnerability, there is a software patch that could be installed to fix the vulnerability and lessen the chance of data being compromised. Just like the SharePoint vulnerability, CVE-2021-0604, the Microsoft Azure vulnerability is also a remote code execution vulnerability. This is a vulnerability that exists throughout Microsoft Azure cloud software. In this vulnerability, there is a remote code execution vulnerability in a which a remote attacker can exploit this flaw by sending a specially crafted request to a vulnerable over a publicly accessible remote management port (Narang, 2021). This is a very severe vulnerability that if not properly patched, it can be exploited and lead to further complications.

**Major Vulnerabilities: Colonial Pipeline Ransomware Attack**

Regarding the Colonial Pipeline ransomware attack, the hackers saw an opportunity and a vulnerability in the system, and they seized it. The year before the Colonial Pipeline attack, the

SolarWinds attack also left a mark on the United States, where attackers hacked into different federal departments and compromised sensitive data (Lazarovitz, 2021). The results of this attack should have been a lesson because of the adverse effects it left on the various federal government agencies. However, due to the failing infrastructure and weak security, the pipeline was hacked, leading to fuel shortages and devasting, long-lasting impacts (Ford, 2021).

In terms of vulnerabilities, reports show that the earliest gathered evidence of compromised data was on April 29, where hackers gained access to the network through a legacy virtual private network and an employee's credentials (Ratnayake, 2021). Unfortunately, the company did not set up simple preventative measures like multifactor authentication, so it took the attacker a minor effort to access the systems and compromise data (Ratnayake, 2021). From this mistake, the attack was then able to access the network and hack into the systems. The severity of the attack forced the largest U.S. oil fuel pipeline to shut down, leading to many people experiencing gas shortages (Eaton, 2021). In addition, the attack should lead others to have an increased awareness of hackers' threats, especially in how poorly secured systems and weak infrastructure are targeted now more than ever.

**Major Vulnerabilities: WannaCry Ransomware Attack**

Regarding the WannaCry Ransomware Attack, there were many vulnerabilities that were found that led to the attack happening. Prior to the occurrence of the WannaCry Ransomware attack, the N.S.A. created Eternal Blue, which was a tool created for cyber-attacks. This tool affected a particular version of the Microsoft Windows Operating Systems and exposed a vulnerability in the system. In addition to affecting the software, any device that uses a Server Message Block protocol is vulnerable to being a victim of various ransomware attacks. While the N.S.A. identified the vulnerability in the S.M.B. protocol years prior, they did not disclose it to

Microsoft because they intended to use it as a cyber tool for their purposes (Hawthorne, 2020). Because the attacker can transmit the malicious code through an open port, they can place a buffer overflow in action. Exploiting a vulnerability in the Server Message Block (S.M.B.) protocol allows ransomware to spread rapidly across a network (McDonald et al., 2022). Due to the vulnerability found in Eternal Blue, the WannaCry Ransomware attack exposed various security threats, stole millions of dollars of assets, and decimated many people's lives. Having unpatched software and open vulnerabilities can lead to much destruction, and individuals and businesses can suffer those consequences.

From outdated software without the appropriate security patches to the N.S.A. having a foreknowledge about the vulnerability, many factors could have led to the attack. The cybercriminals saw an opportunity in the Eternal Blue exploit, taking advantage of the vulnerability in the system. Due to many companies still heavily relying on legacy software and not updating their computers, they can be vulnerable to attacks that can negatively penetrate systems (Taylor & Francis Online, 2017). While it can be a nuisance to update software in systems, it can save a business and organization from massive financial loss if they implement proper security measures and update their systems. Due to this vulnerability, the attacker uses the Eternal Blue exploit to get on the network, spreading the ransomware through exposed S.M.B. ports. In addition to Eternal Blue, the attack used a DoublePulsar backdoor to leverage the MS17-010 SMB vulnerabilities (Akbanov et al., 2019). While the reasoning for these attacks was due to outdated and unpatched software, the N.S.A. takes slight responsibility for this.

As previously mentioned, the N.S.A.'s creation of the Eternal Blue exploits caused massive destruction to various organizations and businesses. Even though attackers go about their attacks in different methods, they can use the N.S.A. tool, Eternal Blue, to infect computers

and spread ransomware (Newman, 2018). Because of this tool, hackers can manipulate the flaws in the Server Message Block to infect computers and execute forms of malicious code on the computer. A couple of months before the WannaCry attack, the N.S.A. could have better informed those who used the older software because they knew about the vulnerability. Instead, the agency cloaked itself in secrecy for years, and officials refused to acknowledge its existence (Zegart, 2017). This mindset is damaging because WannaCry and other ransomware attacks that used Eternal Blue further broke the trust between people and the N.S.A.

**Major Vulnerabilities: Kaseya Ransomware Attack**

Regarding the Kaseya Ransomware Attack, one of the leading causes of this attack was the outdated software and lack of security patches put in place that existed. REvil saw an opportunity in this vulnerability, taking advantage of it and injecting malicious software to MSPs worldwide. At the same time, the code of the software was not compromised; Kaseya's platform that was used to deliver their services was and had ransomware put on it. The Kaseya VSA agent (C:\PROGRAM FILES (X86)\KASEYA\<ID>\AGENTMON.EXE) was deployed to Kaseya's customers (MSPs) and deployed to the MSP customer's systems, which pulls from Kaseya's cloud-based servers (Allen, 2022). While it can be a nuisance to update software in systems, this attack shows how it can be beneficial in the long run and save a business and organization from collateral damage. Businesses can prevent themselves from losing severe amounts of money if they implement proper security measures and update their systems. In the attack, the vulnerability CVE-2021-30116, SQL injection, was exploited by REvil and allowed platform authentication to be bypassed, which gave the attackers maximum privileges (Pelliccione, 2021). Even before a patch could be implemented, REvil had already made its way into the systems, compromising servers and workstations.

## Mitigation Techniques

Throughout the various attacks that occur, understanding what went wrong and the steps that should have been taken can help a business or organization be able to be better prepared. This can also help them further mitigate potential attacks that could arise in the future. Mitigation is defined as the ability taken to reduce or eliminate risk to people and property from hazards and their effects (Bullock et al., 2013). By understanding mitigation techniques, the risk of these attacks can be lessened significantly, and businesses can be able to operate more effectively. There is a major importance of ransomware mitigation towards businesses, and it can be able to serve as a great benefit if done early. By incorporating ransomware mitigation strategies in IoT devices during the entire lifecycle of application execution, it can best protect them from a ransomware attack (Humayun et al., 2021). While these attacks continue to increase, if properly mitigated, they can be controlled and lessened significantly.

One of the main mitigation techniques is making sure that computers and networks are installed correctly. Even though ransomware attacks do not happen to every single company all the time, companies should be prepared for a potential attack. By creating daily or real-time backups of their data, it is an important mitigation tactic to safeguard and protect the important data throughout the organization. Organizations should store the copies of the backups offline to "ensure that ransomware has no access to them, as well as maintaining a "gold image" of system configurations (i.e., one that allows an organization to reset systems to the pre-attack state)" (Singh & Sittig, 2016). Having trained I.T. staff put in place who can restore the backups is important to the health of the overall organization. Furthermore, trained I.T. staff is critical to the organization because they are responsible for maintaining all of the computers' operating systems, application software, browsers and plug-ins, firmware, and anti-virus software should

ensure that they are up to date with the latest patches (Singh & Sittig, 2016). The patches that get installed should not lead to more problems and should be tested thoroughly before getting applied to the system. Additionally, it is important that the network engineers make it a point to ensure that the organization's firewall is properly configured to prevent unauthorized access to the organizational resources (Singh & Sittig, 2016). These changes and policies are important for the well-being of the organizations and if properly implemented, it can reduce the chances of ransomware attacks throughout an organization.

Additionally, control access policies for organizations and businesses should be implemented. For example, there should be restricted access for users to create and remove files from the computer. The business or organization should also consider limiting users' ability to install and run software applications using the principle of "Least Privilege," or minimize users' access to only those systems and services required by their job (Singh & Sittig, 2016). For users who might need administrative access it would be beneficial to have two accounts created for that purpose. In these two accounts, there would be one with administrative privileges that is used only when necessary, and one with restricted privileges, for day-to-day activities, like reading email and browsing the Internet (Singh & Sittig, 2016). As mentioned previously, restricting various access, and creating administrative privileges on local computers is important to safeguard the organization from potential attacks that can occur.

After the networks and computers are properly installed, the next step would be to have informative and engaging security awareness training so that the users throughout the company can know how to properly use their devices and be secured. Since training courses have already been created for security awareness, the business or organization does not have to make their own courses (Singh & Sittig, 2016). Throughout the training process, the I.T. staff must be

willing to work with the users and create a variety of scenarios to prepare the user for a potential attack. I.T. professionals must help create messages such that users can easily recognize them as legitimate e-mails. Specifically, the I.T. staff would help create legitimate emails and send them from the organization's I.T. department, where they would show what a genuine email looks like (Singh & Sittig, 2016). Throughout this email, the goal would be to build trust between the I.T. department and the users, to show them what a genuine email looks like, so they can be more watchful for potential phishing attacks.

By having the users become more watchful of potential attacks, they would be able to better respond to attacks and understand the importance of not opening attachments or links on fraudulent emails. The I.T. staff should conduct simulated phishing attacks by sending fake email messages or links to websites that appear to be from legitimate sources, seeing how the user would respond (Singh & Sittig, 2016). Having the user understand the differences between safe and fraudulent emails is important for them as well as the overall health of the organization. Throughout these trainings, the I.T. staff should increase the user's ability to respond to a successful ransomware attack by periodically conducting mock system recovery exercises (Singh & Sittig, 2016). There should be virus protection installed throughout these systems in order to fully protect and secure the infrastructure, as well as requiring two-factor authentication for all users.

Following the training, it should be imperative for organizations to develop a network and user activity monitoring system that conducts surveillance for suspicious activities (Singh & Sittig, 2016). Monitoring suspicious activity is important because it can detect and analyze if there is a potential threat occurring. Some of these suspicious activities can be a receipt of email messages from known fraudulent sources, executable email attachments, unexpected changes in

key files on network-attached drives, unknown processes encrypting files, or significant increases in network traffic on unexpected ports (Singh & Sittig, 2016). It is important that the organization should constantly monitor the environment around them for vulnerabilities and potential risks that can occur throughout a system. As the I.T. staff in an organization monitors the external environment, there should be periodic identification of the gaps or lack in the research that exists.

By having the network and computers properly installed to using various training protocols to ensuring suspicious activities will be monitored, an organization will be adequately prepared to handle the potential attacks that might occur. When a potential attack like ransomware occurs, there is typically an alarming message sent to the background of computers throughout an organization (Singh & Sittig, 2016). In the case of this attack occurring, the users should understand the proper steps they should take to properly protect themselves and the businesses. The affected users should turn off their computer and report it to their I.T. support team immediately, where the I.T. professionals will disconnect the infected computers from the network and turn off wireless network functionality (Singh & Sittig, 2016). However, if the attack becomes increasingly widespread, both wireless and wired networks should be shut down. Taking proper precautions are important for an organization to survive throughout the increase of the security threats. The organization should also continue to work with their I.T. department as well as external security experts to ensure their systems and security policies have the protective measures put in place.

**Mitigation Techniques: Colonial Pipeline Ransomware Attack**

Regarding the colonial pipeline attack, there are many ways this attack could have been mitigated. To start, if the system were adequately secured and had an increased security method

like multifactor authentication, the hackers would have been less likely to enter the system. Additionally, implementing robust forms of energy storage can play a big part in mitigating damages (Medlock III, 2021). Some mitigation methods are ensuring that passwords are strong and complex, not clicking on suspicious links from unknown sources, using anti-malware software, and not saving your passwords on public computers (Monteith, 2016). While those methods are not guaranteed, companies and users can benefit from lowering their chances of compromised data. Both users and companies need to be aware of the threat that attackers pose and to keep these basic security skills in mind.

From this attacks, the United States government is moving forward and learning from the past. Due to the increasing threat of ransomware and cyber-attacks, The Department of Justice has introduced a Ransomware and Digital Extortion Task Force (DeMarco, 2021). They put this into place because of the cyber-attacks and the rising threat towards the nation's critical infrastructure. In the wake of attacks on the Colonial Pipeline, on June 3, Deputy Attorney General Lisa Monaco issued a Memorandum to federal prosecutors, which would theoretically enhance the Department of Justice's ability to centralize its internal tracking of ransomware attacks (DeMarco, 2021). This mitigation strategy would be vital in fighting against the threat of hackers and the growth of ransomware. It would require all ransomware attacks to be handled in the same way the Department handles terrorism cases (DeMarco, 2021). This type of mitigation strategy is a step in the right direction towards enhanced security and will set a precedent on security measures for the world.

**Mitigation Techniques: WannaCry Ransomware Attack**

As previously explained, even though attacks can have devastating effects on various businesses and organizations, proper security measures can be put in place to mitigate these

threats. Particularly with the WannaCry ransomware, the unpatched software led the attackers to gain access to the system and encrypt the files. If the affected businesses had updated their software to the newer version with the security patch before the attack, there would have been less of a chance for the attacker to compromise the system. Additionally, Microsoft released two products called Defender for Endpoint and Defender for Identity for extensive protection against Ransomware attacks, scoring a 100% in a protection level test (Kapoor et al., 2021). These forms of mitigation techniques can help defend against the attacks that arise.

While it is impossible to build security solutions with complete protection, taking the proper security measures is beneficial. By implementing forms of reverse engineering processes and security applications like Safe Zone, victims can safely return to the last backup logged in Safe Zone and recover the system to its previous state (Kapoor et al., 2021). A business can heavily reduce its risk of being attacked by being proactive with software maintenance and updates, installing anti-malware forms, and ensuring the proper security measures are put in place. Additionally, it is essential that users create strong and complex passwords, not click on suspicious links from unknown sources, and not save their passwords on public computers (Monteith, 2016). The methods discussed can benefit both companies and users and significantly lower their chances of having their data compromised.

**Mitigation Techniques: Kaseya Ransomware Attack**

Regarding the Kaseya Ransomware Attack, the vulnerability in the unpatched software gave the cybercriminals unauthorized access to the V.S.A. system, allowing them to encrypt the files. If Kaseya had updated the software that delivered their products and patched it before the attack, it would have lessened the chances of the attack occurring. Similarly, like the mitigation strategy discussed for the WannaCry Ransomware attack, a company could use two products for

mitigation throughout their computers in their organization: Defender for Endpoint and Defender for Identity. Implementing these products can be beneficial towards an organization or business and can be able to help better protect them from attacks.

## Ethical Component

Ethically, it is critical for those in the cybersecurity field to protect themselves, the data they interact with, and those they serve. They must ensure that even though they have a similar knowledge base as the attackers, they must be ethical in their actions. From a business standpoint, trust must be established between a client and the company; cyber security professionals ensure their clients that their data is appropriately secured. Some ethical principles like protecting subjects from harm and respecting privacy are important considerations that need to be understood (Macnish & van der Ham, 2020). Respect for Persons or Informed Consent must also be applied when dealing with security (Macnish & van der Ham, 2020). Keeping these essential ethical considerations in mind is beneficial when dealing with critical data.

The business must determine if it is morally right to pay the ransom after a ransomware attack. In a ransomware incident, decision-makers must choose whether to pay after weighing all available recovery methods. After all recovery options have been considered, decision-makers must decide whether to pay in a ransomware incident (Hofmann, 2020). Because of this decision's uncertainties, some businesses may find themselves in an ethical bind. Even though it is unclear whether or not the corporation will be able to retrieve its data fully, it is crucial to act morally moving forward once a business is attacked in order to prevent similar attacks from happening in the future.

Additionally, to protect the sensitive data and be ethical towards systems, having a proper set of moral values as an employee and manager of data is critical. Security experts must make sure to implement fundamental ethical principles in their technical products in order not to cause harm or have any negative effect on their users (Kozhuharova et al., 2022). Security is a crucial component in having a well-made system beneficial to both the company and the person storing the information. When it comes to critical data like banking information to credit card information, companies and users need to have the reassurance that their data is adequately protected in addition to the two-factor authentication or changing passwords. When a company is managing sensitive data, it is important for them to be ethically responsible with the data they are interacting with.

**Ethical Component: Colonial Pipeline Ransomware Attack**

In the pipeline attack, there many different ethical decisions that needed to be made throughout the process. It was evident that due to the failing infrastructure and weak security, the pipeline was hacked, leading to fuel shortages and devasting, long-lasting impacts (Ford, 2021). From this attack, there were ethical decisions that were needed to be made in order for the pipeline to continue to function. The attack heavily impacted the oil supply market, and it exposed many security vulnerabilities in the energy infrastructure. A significant shift in the transportation and movement of oil supply throughout the country led to an ever-increasing gas price, with people still feeling the consequences of this attack. Ethically, the I.T. team needed to make various calls and understand the risks that were at hand. Other companies and businesses should see the devastating effects of this attack and then increase security protocols.

**Ethical Component: WannaCry Ransomware Attack**

Businesses that suffered from the WannaCry attack were financially hit, and their need for proper security increased. After assessing the vulnerability in the software, it would have been an ethical move of the N.S.A. to inform those businesses who used the older software because they knew about the vulnerability. Instead, the agency cloaked itself in secrecy for years, and officials refused to acknowledge its existence (Zegart, 2017). Unfortunately, these ransomware attacks further broke the trust between people and the N.S.A. While it is a difficult decision for a group like the N.S.A. to make, reporting the incident earlier would have been an ethically minded decision.

**Ethical Component: Kaseya Ransomware Attack**

As mentioned previously, after a ransomware attack, the business must decide whether it is an ethical move to pay the ransom. After all recovery options have been considered, decision-makers must decide whether to pay in a ransomware incident (Hofmann, 2020). Regarding the Kaseya ransomware attack, there were calls that needed to make for the well-being of the organization. This call can be an ethical dilemma for some businesses because of the uncertainty that exists. While there is a general amount of uncertainty of the likelihood of recovering data, the ethical decision should not be considered lightly. There should be an understanding established that the compromised organization or business might not be able to fully recover their data, and they could be more prone to more attacks. Regardless, after a business gets attacked, it is vital to make the ethical choice to move forward and prevent attacks like this from occurring in the future.

## Conclusion

Throughout time, as shown, technology is continuing to have a significant impact on the lives of individuals and is rapidly changing each day. While there is an increase in the accessibility of technology, cyber-attacks are becoming increasingly prevalent. Looking at the three case studies of ransomware attacks, it is apparent in how ransomware has had an impact all throughout the world. With the rapid change of technology, there is an increase in the risk of being a victim of a cyber-attack. From studies to numerous reports, much research has shown the immense impact ransomware has on various organizations and businesses. As time increases, cybercriminals become increasingly deceitful in their hacking techniques, leading to further damage. From mismanaged security settings to numerous vulnerabilities to outdated software, many factors cause ransomware attacks to occur. The attacks that occurred as well as potential attacks can be mitigated by urging the public to be increasingly aware of the threats and implementing proper prevention techniques. As technology is becoming more ingrained in our everyday lives, businesses and individuals must be mindful of the security threats and implement proper security protocols.

## References

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy006

Akbanov, M., Vassilakis, V. G., & Logothetis, M. D. (2019). WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. *Journal of Telecommunications and Information Technology*, *1*(2019), 113–124. https://doi.org/10.26636/jtit.2019.130218

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*. https://doi.org/10.3389/fcomp.2021.563060

Allen, J. (2022, June 15). *Kaseya Ransomware Attack Explained By Experts*. PurpleSec. Retrieved November 15, 2022, from https://purplesec.us/kaseya-ransomware-attack-explained/#Responded

Andrew Sears, A. (2021). Ransomware: A bibliometric research study. *SLIS Connecting*, *10*(2), 73–81. https://doi.org/10.18785/slis.1002.08

Andronio, N., Zanero, S., & Maggi, F. (2015). HelDroid: Dissecting and Detecting Mobile Ransomware. In *Research in attacks, intrusions, and defenses* (Vol. 9404, pp. 382–404). essay, Springer International Publishing.

Arachchilage, N. A., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38,* 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Arunlal, K. S. (2019). Impact of malware in modern society. *International Journal of Scientific Research and Engineering Development, 2*(3), 593–600.

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security, 111,* 102490. https://doi.org/10.1016/j.cose.2021.102490

Brewster, T. (2017, May 15). *Microsoft just took a swipe at N.S.A. over the wannacry ransomware nightmare*. Forbes. Retrieved April 11, 2022, from https://www.forbes.com/sites/thomasbrewster/2017/05/14/microsoft-just-took-a-swipe-at-nsa-over-wannacry-ransomware-nightmare/?sh=1d1f34743585

Brooks, C. (2022, October 12). *Cybersecurity in 2022 – a fresh look at some very alarming stats*. Forbes. Retrieved March 6, 2023, from https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=5018c5b06b61

Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2013). Mitigation, prevention, and Preparedness. *Introduction to Homeland Security*, 435–494. https://doi.org/10.1016/b978-0-12-415802-3.00010-5

Demarco, E. J. (2021). OCC WARNS AGAINST RANSOMWARE. *The R.M.A. Journal*. Retrieved November 15, 2021, from http://bi.gale.com/global/article/GALE%7CA676920221?u=vic_liberty.

Eaton, C. (2021). Colonial Pipeline Hack: How Have Gas Prices Been Affected and Who Are the Darkside Cyber Attackers? Assault forced the shutdown of the nation's largest fuel pipeline to the East Coast over the weekend. Wall Street Journal (Online).

Ehrenfeld, J. M. (2017). Wannacry, cybersecurity and health information technology: A time to act. *Journal of Medical Systems*, *41*(7). https://doi.org/10.1007/s10916-017-0752-1

Ford, E. W. (2021). Cyber ransom in the information age: A call to arms against the hackers. *Journal of Healthcare Management, 66*(4), 243–245. https://doi.org/10.1097/jhm-d-21-00161

Graham, K. (2022). *Top 7 Ransomware Attack Vectors and How to Avoid Becoming a Victim*. BitSight. Retrieved 2023, from https://www.bitsight.com/blog/top-7-ransomware-attack-vectors-and-how-avoid-becoming-victim

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity*, *3*(1). https://doi.org/10.1093/cybsec/tyw018

Haney, J., & Lutters, W. (2020). Security awareness training for the workforce: Moving beyond "check-the-box" compliance. *Computer*, *53*(10), 91–95. https://doi.org/10.1109/mc.2020.3001959

Hawthorne, M. (2020, October 29). *What is EternalBlue?* Technipages. Retrieved April 11, 2022, from https://www.technipages.com/what-is-eternalblue

Hofmann, T. (2020). How organisations can ethically negotiate ransomware payments. *Network Security*, *2020*(10), 13–17. https://doi.org/10.1016/s1353-4858(20)30118-5

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105–117. https://doi.org/10.1016/j.eij.2020.05.003

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: A review and future directions. *Sustainability*, *14*(1), 8. https://doi.org/10.3390/su14010008

Kerner, S. M. (2023, January 26). *Ransomware trends, statistics and facts in 2023*. Security. Retrieved 2023, from https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts#:~:text=According%20to%20the%202022%20%22Verizon,State%20of%20Ransomware%202022%22%20report.

Kozhuharova, D., Kirov, A., & Al-Shargabi, Z. (2022). Ethics in cybersecurity. What are the challenges we need to be aware of and how to handle them? *Cybersecurity of Digital Service Chains*, 202–221. https://doi.org/10.1007/978-3-031-04036-8_9

Lazarovitz, L. (2021). Deconstructing the solarwinds breach. Computer Fraud & Security, 2021(6), 17–19. https://doi.org/10.1016/s1361-3723(21)00065-8

Macnish, K., & van der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in Society, 63,* 101382. https://doi.org/10.1016/j.techsoc.2020.101382

McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J., & Buchanan, W. J. (2022). Ransomware: Analysing the impact on windows active directory domain services. *Sensors*, *22*(3), 953. https://doi.org/10.3390/s22030953

McIntosh, T., Kayes, A. S., Chen, Y.-P. P., Ng, A., & Watters, P. (2022). Ransomware mitigation in the modern era: A comprehensive review, research challenges, and Future Directions. *A.C.M. Computing Surveys, 54*(9), 1–36. https://doi.org/10.1145/3479393

Medlock III, K. B. (2021, May 11). The Colonial Pipeline Outage: An important lesson for U.S. Energy Security. *Forbes.* Retrieved November 15, 2021, from https://www.forbes.com/sites/thebakersinstitute/2021/05/11/the-colonial-pipeline-outage-an-important-lesson-for-us-energy-security/?sh=4231ec2726ef.

Monteith, B. (2016). Hacking for Good and Bad, and How to Protect Yourself against Hacks! *Knowledge Quest*, *44*(4), 60–64. Retrieved 2021, from http://ezproxy.liberty.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fhacking-good-bad-how-protect-yourself-against%2Fdocview%2F1770514318%2Fse-2%3Faccountid%3D12085.

Narang, S. (2021, October 5). *CVE-2021-38647 (OMIGOD): Critical Flaw Leaves Azure Linux V.M.s Vulnerable to Remote Code Execution*. Tenable®. Retrieved 2023, from https://www.tenable.com/blog/cve-2021-38647-omigod-critical-flaw-leaves-azure-linux-vms-vulnerable-to-remote-code-execution

Newman, L. H. (2018, March 7). *The Leaked N.S.A. Spy Tool That Hacked the World*. Wired. Retrieved 2022, from https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/

Pelliccione, A. (2021, July 5). *The ransomware threat rises to the next level: the Kaseya case, how it happened and how to defend yourself*. Agenda Digitale. Retrieved 2022, from https://www.agendadigitale.eu/sicurezza/la-minaccia-ransomware-sale-di-livello-il-caso-kaseya-come-successo-e-come-difendersi/

Pranggono, B., & Arabo, A. (2020). Covid-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2). https://doi.org/10.1002/itl2.247

Ramel, D. (2023, January 17). *2023 Data Protection Report: 'Ransomware is Winning'*. Virtualization Review. Retrieved 2023, from https://virtualizationreview.com/articles/2023/01/17/data-protection-report.aspx

Ratnayake, D. (2021). Insight: Cybersecurity. ITNOW, 63(3), 39–39. https://doi.org/10.1093/itnow/bwab082

Sahi, S. K. (2017). A study of wannacry ransomware attack. *International Journal of Engineering Research in Computer Science and Engineering*, *4*(9).

Shah, N., & Farik, M. (2017). Ransomware-threats, vulnerabilities and recommendations. *International Journal of Scientific & Technology Research*, *6*(6), 307–309.

Singh, H., & Sittig, D. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied Clinical Informatics*, *07*(02), 624–632. https://doi.org/10.4338/aci-2016-04-soa-0064

Smart, W. (2018). Lessons learned review of the wannacry ransomware cyber attack. *N.H.S. Department of Health & Social Care*, 1–42.

Stephens, T. G. (2021). Lessons learned: The colonial pipeline ransomware attack. California C.P.A.

Taylor & Francis Online (2017). The wannacry ransomware attack. *Strategic Comments*, *23*(4), vii-ix. https://doi.org/10.1080/13567888.2017.1335101

Tiwari, V. K., & Dwivedi, R. (2016). Analysis of cyber attack vectors. *2016 International Conference on Computing, Communication and Automation (ICCCA)*. https://doi.org/10.1109/ccaa.2016.7813791

*Top critical vulnerabilities used by ransomware groups*. SOCRadar® Cyber Intelligence Inc. (2022, November 7). Retrieved 2023, from https://socradar.io/top-critical-vulnerabilities-used-by-ransomware-groups/

Trautman, L. J., & Ormerod, P. (2019). Wannacry, ransomware, and the emerging threat to corporations. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3238293

Voas, J., Kshetri, N., & DeFranco, J. F. (2021). Scarcity and global insecurity: The semiconductor shortage. *I.T. Professional, 23*(5), 78–82. https://doi.org/10.1109/mitp.2021.3105248

Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports, 4*, 100126. https://doi.org/10.1016/j.chbr.2021.100126

Yuryna Connolly, L., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity, 6*(1). https://doi.org/10.1093/cybsec/tyaa023

Zegart, A. (2017, June 29). *The N.S.A. Confronts a Problem of Its Own Making*. The Atlantic. Retrieved 2022, from https://www.theatlantic.com/international/archive/2017/06/nsa-wannacry-eternal-blue/532146/