**Final: The Colonial Pipeline Critical Incident V2**

Robert Chapa

Saint Leo University

Dr. Todd Isaacson

December 15, 2021

**Author Note**

Robert Chapa

I have no known conflict of interest to disclose.

Email: [bobby.chapa@gmail.com](mailto:bobby.chapa@gmail.com)

**Table of Contents**

Abstract……………………………………………………………………………………3

Introduction……………………………………………………………………………….4

Stakeholders……………………………………………………………………………....9

Critical Review of Related Literature…………………………………………………….15

Ransomware……………………………………………………………...…………...….33

DarkSide…………………………………………………………………………………33

Colonial Pipeline Mitigation Preparedness Phase….……………………………………34

Colonial Pipeline Mitigation Response Phase……………………………………………35

Colonial Pipeline Mitigation Recovery Phase……………………………………………36

Conclusion...……………………………………………………………………………..39

Stakeholders Map………………………...………………………………………………40

References…………………………………..……………………………………………41

DCJ 710 Project Colonial Pipeline

**Abstract**

The purpose of this paper is to evaluate the mitigation in preparation, response, and recovery of the Colonial Pipeline critical incident. Although the company had experienced a ransomware attack the previous year, suitable security protocols were not. Due to lack of staffing, the TSA had not updated cybersecurity regulations regarding pipelines. Members of Congress have submitted that the TSA should increase its funding to deal with cybersecurity threats. Another suggestion has been to remove the TSA from its authority over pipelines to a better-suited government authority. Pipeline security is a recommended procedure and is not mandatory. The lack of compulsory security implementations has caused concern among members of Congress. As of the current date, Congress has not taken significant action.

*Keywords:* Colonial Pipeline, ransomware, cybersecurity, oil, hacker, virus, computer

**Introduction**

The Colonial Pipeline company experienced a ransomware cyberattack on May 8, 2021. The attack prompted the company to halt the pipeline operation, disrupting gasoline and other refinery products. The attack caused a significant petrol disruption along the East Coast. The assault was the second ransomware attack that disrupted Colonial Pipeline operations in the last two years. The company had experienced a cyber-attack on Communications Systems in 2018. Because of the critical nature of delivering refinery products, the Colonial Pipeline remains a high-value target for malicious actors (Parfomak & Jaikaran, 2021).

This paper will examine the Colonial Pipeline, critical incident in detail using the Nunez and Vendrell (2017) paradigm of three phases of mitigation: planning, response, and recovery. Then the company's actions during the assault will be specifically discussed. Lastly, security improvements and review barriers to implementation will be proposed.

All pipelines in the United States are part of the surface transportation critical infrastructure. The transportation security ministration TSA administers security for the sector, a Department of Homeland Security sub-organization. The TSA testified to Congress, but cybersecurity threats are outpacing the ability to write and disseminate regulations to address the attacks. The problem is partly due to inadequate staffing, outdated risk assessments, and a lack of certainty or understanding of the effectiveness of security standards (Parfomak & Jaikaran, 2021).

Pipeline security has several elements that can be a broad topic of research—the purposes of this paper. This paper will present research on the government's position on pipeline security before the Colonial Pipeline attack. An examination of the main concerns and threat vectors that legislatures are fearful of regarding pipeline security and then discuss how those views and circumstances change in the advent of cyber warfare. It will be fascinating to see what legislatures have done since this attack to enhance the security of pipelines. All these examinations will use the critical incident management system.

Additionally, research on the conduct of the Colonial Pipeline after the first ransomware attack in 2019 will be done. The questions will be: What security changes were made to prepare for the next episode? Did Colonial implement the planned changes to security? Did Colonial heed the recommendations from the TSA regarding protection?

Furthermore, a look at mitigation in the recovery efforts of the Colonial Pipeline will be reviewed. What has changed since the ransomware attack? Has the company implemented the TSA security measures? Has there been a federal audit of the security protocols and mitigation response?

Darkside's disruption of the eastern seaboard will also be examined. After the Colonial pipeline shut down pipeline operations, the impact was immediately visible by the long lines of customers at gas stations. There was also an increase in the price of gas. Flight stoppages and customer anxiety impacted business throughout the eastern coast (*Colonial Pipeline Co. attack: What really happened*, 2021). A successful attack like this has a psychological impact on the population. It quickly becomes apparent how delicate our economic society is.

The criminal actor in the Colonial Pipeline cyberattacks chose to use malicious software known as ransomware. Ransomware falls under a type of malware known as a worm. This type of malware propagates through a network, infecting systems as it moves along. If the malware finds the kinds of file folders that hold viable data, it will encrypt those files and lockout the users. Afterward, messages are sent to the victims asking for the key to decrypt their systems. The price is usually required in cryptocurrency, so that it is difficult to trace. Ransomware used on Colonial Pipeline was known as Darkside or ransomware as a service (RaaS). The ransomware is a cybercrime model that hacker groups develop, host the infrastructure, and then charge another criminal organization to utilize their services to conduct a cyberattack (Parfomak & Jaikaran, 2021).

This paper will examine ransomware extensively to create mitigation response and recovery plans. Its origins, method of attack, and likely threat vectors will be introduced.

A proposal for mitigating ransomware in the three phases will be offered. The vulnerabilities the Colonial Pipeline has are the same for any other industry. Therefore, it is likely that other companies that have successfully mitigated a ransomware attack may apply to the Colonial Pipeline.

To understand the threat that ransomware poses to the industry. It is also important to review or carefully examine the organization Darkside. Discussion of the following questions: who is Darkside? Why does it exist, and who uses it? Other questions will focus on what is the government doing to address the threat of ransomware as a service?

These questions will be reviewed through the three-phase critical incident management methodology lens. The primary concern is in the mitigation preparation phase. This is most important because these attacks have continued to increase with no signs of slowing.

Virtual private network VPN will also need to be discussed in this paper. Through a VPN, Darkside was able to attack with its ransomware virus. VPNs are a critical threat vector because everyone uses them. Therefore, it is crucial to understand what mitigation efforts have taken place to prepare for the next ransomware threat (*Colonial Pipeline Co. attack: What really happened*, 2021).

In the case of the Colonial pipeline, the system administrators failed to implement solid password security protocols. Darkside identified and then used an outdated VPN account to launch their attack. The older VPN account had been part of a more significant cache of compromised passwords available on the darknet (*Colonial Pipeline Co. attack: What really happened*, 2021).

The compromise of the VPN account leads to the next topic of discussion—two-factor authentication. If Colonial pipeline had enforced two-factor authentication for their VPN access, DarkSide would not have been able to use this threat vector to launch their attack. It is estimated that without two-factor authentication, the success rate for using purchased credentials on the dark web is high at 20 to 50% success using a compromised credential. Couple this with the fact that the effort using the credentials is low, and you have a recipe for continued attacks by malicious actors (*Colonial Pipeline Co. attack: What really happened*, 2021).

An interesting mitigation tactic during the response phase is the inclination of organizations to pay the ransom. A look at the benefit-cost analysis of paying—the ransom and the civil and criminal liabilities accompanying the payment will be made. In the case of the Colonial Pipeline, the company paid $4.4 million to the malicious actors. The Department of Justice successfully recouped 2.3 million in bitcoin (*Colonial Pipeline Co. attack: What really happened*, 2021).

Even though the ransomware attack impacted the East Coast and caused gas prices to rise by 4%, the Colonial Pipeline did do some things correctly in its mitigation response phase. It is essential not to ignore this fact and examine and reinforce the correct behavior. An exploration of this behavior will be in-depth and discuss areas of improvement. An example of something done correctly by the Colonial Pipeline was that they reported the incident quickly to the FBI. The authorities promptly contacted the Internet service provider ISP and isolated the servers holding the uploaded information by the malicious actors. Because of this quick action, the malicious actors lost access to over 100 GB of data stolen from the Colonial Pipeline. This critical incident would have been far worse (Pankov, 2021).

The federal government response was swift. President Biden deserves credit for a fast and broad response to the attack. His administration put into action many directives. Primary was the focus on keeping fuel flow to all affected communities (*Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*, 2021). This mitigation during the response phase saved millions of dollars and probably lives. President Joe Biden's response and commitment to fighting cybercrime will be examined. It should be interesting to note if past federal responses from different administrations were as quick to action.

A unique action by the federal government during the recovery phase was reminiscent of the old west's slogan of 'Wanted dead or alive.' The State Department created a bounty of $10 million for any information leading to the identity or location of the ransomware cybercriminals (Lyngaas, 2021).

The use of bounties to identify and apprehend cyber criminals was powerful. The use of bounties to mitigate the response and recovery phase will be examined. Is this useful and appropriate? Does it work? An investigation into a few relevant bounties issued in the past for cybercrimes to judge their effectiveness will be examined.

The last section of this paper, before the concluding section, will look forward to the evolution of cyber-attacks on critical infrastructure. Additionally, the dangers of open-source knowledge and software will be examined to a limited extent.

The main terrorist threat vectors that exist today are ransomware-style attacks on business and financial institutions along with physical types of machinery such as drones or other nanotechnologies in the hope of damaging critical infrastructure. The potential for these types of attacks on our infrastructure far outweigh hurricanes or any other natural disasters.

The concluding section of this paper will review all mitigation actions from both Colonial Pipeline and the federal government in their planning, response, and recovery phases. Lessons learned and current legislation regarding the impact of ransomware on infrastructure will be reemphasized. Cybersecurity best practices will be re-stated.

**Stakeholders**

The stakeholders are displayed in a stakeholders map in a later section of this paper. In this section, the different stakeholders will be discussed. Several main elements were identified and then organized into four quadrants: public quadrant, criminal quadrant, Colonial systems quadrant, and federal government. The first quadrant to be discussed is the criminal quadrant.

Russia is the main element here because of its state-sponsored cybercriminal actions. According to Microsoft, Russia primarily targets the US. In the last year, 58 percent of cyberattacks detected by Microsoft originated in Russia. This increased 52% from the previous year (*Microsoft digital defense report*, 2021).

A sub-system of Russia is its foreign intelligence service (SVR). It has a process that coordinates with the Russian military agency (GRU). These two systems and the domestic security service (FSB) have processes between the three to engage in cyber operations. Furthermore, Russia has a process where it finances and supports with technical expertise cybergangs such as 'Revil.' (*Microsoft digital defense report*, 2021).

The Dark web is an element of the criminal quadrant. It has a marketplace for the purchase of several cybercrime services. A cybercriminal gang may purchase services such as ransomware kits for as little as $66. They may also buy compromised PCs for launching attacks for as little as 13 cents. Denial of service attacks is available for $311.88. In the Colonial Pipeline ransomware attack, the stolen username and password pairs may be purchased for 97 cents or $150 for 400 million; as can be seen from these numbers, the illicit market makes the cost of an attack very cheap. The cost-benefit is favorable for a cybercriminal (*Microsoft digital defense report*, 2021). The Dark web element has a relationship with the state-sponsored cybergangs via the supply of cybercrime services.

The DarkSide element offered ransomware as a service (Raas) via the dark web. Through the DarkSide Raas element, the cybercriminal gang Revil compromised the Colonial Pipeline servers and databases (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

Revil is an element in the Criminal quadrant because the cybercriminal gang financed by Russia attacked Colonial Pipeline. Revil purchased a set of credentials from the Dark web marketplace and used DarkSide RaaS to administer the attack. Thus, the relationships between all four entities have been completed (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

The next quadrant is Colonial systems. Here we find the elements, employees, IT administrators, and Leadership team. The first element to be discussed is the Employees. The Employees element was very significant because an IT staff member found the first vulnerability. A previous Colonial employee who had VPN access at one point made the mistake of using the same password for different access credentials other than at work (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

The IT element maintains computer assets, information, and computing infrastructure. Computer assets consist of routers, networks, and computing machines. Because these systems are connected to the internet, they provide additional vectors for a compromise (Johnson, 2015).

A malicious actor likely discovered the password on a different platform that was easier to hack or compromise. The password was listed on the Dark web. Revil searched for the valuable compromised password, purchased it, and then added it to the attack strategy. If the employee had followed reasonable password procedures by having different complex passwords for each account, then the attack via this vector would not have been possible (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

Enter the Colonial IT Administration element. The real culprit is the IT security administrator who was too busy to follow suitable server administration protocols and disable former employees' VPN access credentials. Had this one crucial step been completed, then this vector would have been shut down (Turton & Mehrotra, 2021).

The second criticism of the Colonial IT administration was their failure to maintain air-gapped backups. IT department that practices this security measure has secure backups that cannot be encrypted via ransomware (Johnson, 2015).

The last element in the Colonial quadrant is the Leadership Team. The leadership element consists of the CEO, the board, directors, and owners. They make all the administrative decisions regarding the company's operations. They maintain communication and supervision of the IT team and other departments.

Administrators made sound decisions once informed of the ransomware attack. Although they did pay the 5-million-dollar ransom, they also contacted authorities. This fast communication allowed the authorities to act and recover some of the ransom (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021).

Additionally, the administration quickly shut down the pipeline, showing excellent leadership (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

Probably the essential quadrant is the Federal Government. It consists of several elements that played a role in the Colonial Pipeline critical incident. The elements were the US Justice Department, 'other agencies,' the US State Department, the US Military, the FBI, the US President, Congress, and the TSA. All these elements have relationships with each other for making decisions and executing the orders of the President and Congress, thus impacting all of the other quadrants (*Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021).

The President has the authority to mobilize a robust federal response. The response may include establishing interagency groups to monitor and ensure that resources are available to the impacted communities. Federal laws and regulations can also be temporarily lifted by the President (*Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*, 2021).

Congress is an equally important element that passes laws, provides funding, and determines which government agencies are accountable for pipeline supervision and regulation enforcement. The processes and communications flow in both directions from Congress to the entities in this quadrant (*Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*, 2021).

The US Military, 'other agencies,' the TSA, and the US Justice Department have assets to engage the enemy with counter cyber-attacks or other direct means. They follow the order of the President and maintain processes and flow of communication between the President and each other during a critical event. These departments worked together to attack Revil and DarkSide, impacting their operations and funding (Chipolina, 2021; *Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*, 2021; Menn & Bing, 2021).

The US State Department executed another mitigation effort. They issued a bounty of 10 million dollars for information leading to actionable intel on DarkSide Revil or anyone else involved in the Colonial Pipeline incident. Of course, the State Department maintains processes and information flow with the President and Congress (Chipolina, 2021; *Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*, 2021; Menn & Bing, 2021).

The last element in this quadrant is the TSA. This agency currently has the authority over pipeline laws and regulations. They oversee all critical incidents regarding pipelines and can enforce policies. During the Colonial Pipeline incident, they maintained processes and flows between Colonial and the other elements in the Federal Government quadrant (*Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021).

The public quadrant is the final one to be discussed in this stakeholders map. It is arguably the most important one. All the other quadrants exist to serve or hurt the public quadrant. It contains five elements.

The first one is the private businesses that provide goods and services to the general public. Businesses depend on the oil supplied from the Colonial pipeline to supply fuel for the delivery vehicles that serve them with goods. The oil also provides fuel to their customers whom businesses serve and depend on for sales (*Colonial Pipeline Co. attack: What really happened*, 2021; Parfomak & Jaikaran, 2021).

Within the public quadrant exist the US eastern states that were also impacted by the interruption of fuel flow. Similarly, these states depend on fuel proved by the Colonial pipeline to serve and protect the communities with their boundaries. This includes police and fire departments, judicial functions, and many other sub-systems, each with its processes.

The news media is an element that heavily impacts all the other elements in this quadrant due to the news and how it provides it. A breach such as the Colonial Pipeline could be reported negatively, causing fear and psychological damage to the general population, making the job of the other elements more difficult.

Private citizens are the essential elements in this quadrant. They are impacted by the elements and suffer if fuel becomes unavailable. They depend on fuel for employment, home heating, food, medicines, etc. Without sufficient fuel, even the hospitals will eventually be unable to provide services resulting in the loss of life (*Colonial Pipeline Co. attack: What really happened*, 2021; Parfomak & Jaikaran, 2021).

Lastly, informants are an element. They may have actionable intelligence about persons, organizations, or crimes that the government may use to arrest and prosecute those responsible. In the Colonial Pipeline incident, they are being incentivized with the offer of millions of dollars in bitcoin (Lyngaas, 2021).

In conclusion, several elements have many processes in the Colonial Pipeline ransomware incident. All quadrants have elements that were impacted by the breach. The fallout of this breach is still ongoing. How will many persons with compromised sensitive data be impacted by stolen identities or other credit issues?

**Critical Review of the Literature Course Project**

In May 2021, the Russian cybercriminal gang 'Revil' attacked the Colonial pipeline with a ransomware cyberattack that forced production to shut down. This attack disrupted oil flow and other business processes throughout the eastern seaboard. The following article focuses on the US government's response to this attack (Menn & Bing, 2021).

The authors report that there has been a paradigm shift in how the US government handles hacking organizations. Cyberattacks on critical infrastructure are now going to be treated similar to terrorism. This shift is credited to US Deputy Attorney General Lisa Monaco. The Justice Department and other agencies now have a legal right to request assistance from US intelligence agencies and the Department of Defense (Menn & Bing, 2021).

Armed with this legal basis, the US engaged in cyber warfare against the criminal hacker group reveal. This attack forced the hacker group's business websites offline and the newsgroup's leading spokesman to go into hiding. The FBI, the Cyber Command, the Secret Service, and other countries with disruptive services by these groups conducted this attack. The author attempted to remain neutral in reporting the government-sanctioned attack on evil. However, the article's tone indicates that they are very much in favor of state-sponsored cyber warfare on cybercriminals (Menn & Bing, 2021).

Research in this article focused on the response by American law enforcement to the Russian lead criminal cyber warfare gang that conducted the cyber attack on the Colonial pipeline last May. According to the authors, US authorities used military and other agencies to conduct a state-sponsored cyber attack. With the assistance of the military and other agencies, the US authority was able to cause damage to Revil servers. The authors state that other entities and countries were protected from further cyber-attacks (Menn & Bing, 2021).

This proactive approach also enabled the FBI to obtain the universal decryption key, which allowed the colonial pipeline to recover much of the ransomware and many additional files without paying more. Due to the success of hacking the cybercriminal's servers, US authorities could load their applications within the hacker servers when the system administrators turned them back on. They could do this because the government hackers had compromised the backups (Menn & Bing, 2021).

The authors did an excellent job discussing some of the technical processes that led to US authorities compromising Revil's servers. Discussion about the advantages of forcing Revil offline and protecting future victims was also discussed. However, there was no discussion about the possible complications if this offense of posture violates existing international laws. Although, they can be applauded for the taken offense at the approach. This may escalate or provoke attacks on more critical infrastructure such as hospitals or the electric grid of states that require air conditioning. There is also the possibility of American hackers being charged in foreign courts for breaking international law.

A lesson learned is that whether you are the good guys or the bad guys, it would be best to keep your backups safe. This comes into the planning and preparation phase of the critical incident. All organizations should ensure that they have accurate backups that are disconnected from the network to avoid inheriting the ransomware encryption hack (Menn & Bing, 2021). An opportunity to continue support government efforts to counter-attack and disrupt cybercriminal organizations exits. There must be consequences for attacks on our infrastructure.

A possible violation of international law is a potential barrier to implementing this new paradigm shift of taking the gloves off and hitting back with assets that we have not used in the past. Unintended consequences may have a blowback on our culture and society if the United States appears not to respect international law. An unintended consequence might be that US military members or other assets are prosecuted for computer crimes in other countries. Additional information about the actions taken by the federal government is examined in the Fact Sheet issued by the White House on May 11th, 2021.

President Joe Biden responded quickly to the colonial pipeline incident on May 11, 2021. He issued a statement authorizing federal funds and strengthening law enforcement. He promptly addressed the ransomware attack. This mitigation action during the response phase was responsible for saving millions of dollars. The state department quickly created a bounty system. It authorized a $10 million reward frank formation leading to the identity and or location of the ransomware criminal gang (*Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*, 2021).

Another mitigation effort was establishing an interagency response group that monitored and addressed the situation. Mitigation efforts also included waivers to provide flexibility to drivers transporting fuel. And other state requirements were temporarily lifted to ease the burden of the oil disruption. Lastly, the administration issued guidance for industries to secure critical infrastructure. The author was a writer of the federal government who wrote this as a facts-only document. The position was to relay information from the President to the public (*Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*, 2021).

The President's first action to address this issue was establishing an interagency response group. This group had the responsibility of monitoring and managing the situation in real-time. The main objective of this group is to re-establish the fuel to flow to the impact of communities. This was an excellent mitigation response that is assisted businesses to stay functional. An additional mitigation response was for the government to allow one-week waivers to states for the allowance of non-compliant fuel. This effort provided fuel for impacted communities (*Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*, 2021).

Many other mitigation efforts focused on waving truck and transportation regulations temporarily to assist with fuel transport. One of these mitigation factors was the relaxation of operator qualification rules that allowed emergency personnel to be used as a partial return to service (*Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*, 2021).

Additionally, the guidance on securing critical infrastructure was meant to assist all essential infrastructure owners prevent a ransomware Darkside attack. This included sharing information very quickly about the attacks and how they function. The administration provided rapid information to all parties involved in the attack.

The administration did an excellent job with their mitigation response. Everything that was done was for the continuation of fuel to mitigate the impact of the oil disruption. This notice was sent out quickly, and the trouble of oil flow was handled soon asserts that the mitigation efforts were appropriate and prepared to be implemented promptly. As this was a fact sheet, it is impossible to analyze the author's logic or conclusions.

A lesson learned was that planned mitigation efforts for critical infrastructure attacks work. The oil disruption to the eastern states could have been catastrophic. An opportunity that came from this factsheet was that fast communication from the administration to the public eases tensions and anxieties. A strength to be realized was that mitigation efforts during the planning and response phase are very effective if championed at the highest levels. A different research article also discussed a deeper look at the administrations' use of bounties.

This article focused on the US government's response to the colonial pipeline ransomware attack. The mitigation response was the $10 million bounties for any information leading to the identity and location of anyone involved in this incident. The article also discusses some of the strategies by the US government on ransomware tax, such as focusing its attention on how ransomware operations are funded. The report also discussed Russia's role in funding or supporting hacker criminal groups (Lyngaas, 2021).

The author is a writer for CNN and focused on supplying factual information without making opinions. However, through the tone of his writing. It appears that he is a strong proponent of cybersecurity and mitigation efforts during the recovery phase (Lyngaas, 2021).

The authors discussed the $10 million bounty and the recovery mitigation efforts by the Justice Department in recovering money from Darkside. He mentions the government's focus on funding sources for ransomware operatives. However, he does not go into much detail other than to say the Russian government is involved. It would have been good to have more factual evidence about why our intelligence agencies believe this (Lyngaas, 2021).

Some discussion about a decrease in ransomware activity since Biden met with Putin was present. However, it is difficult to say if the Biden visit was the cause of the ransomware suppression. There was light discussion about cybercriminal operatives being pursued outside of the borders of Russia. This would've been an excellent area to delve deeper into how we are doing this and its effectiveness in curbing ransomware attacks.

Lastly, It would be nice to know if the bounties have worked. Have there been any arrests or convictions because of the large bounties? A lesson learned could be that diplomacy may impact state-sponsored cybersecurity attacks. Another lesson could be that taking a proactive approach by targeting the funding sources of cyber gangs may be a good form of mitigation during the planning phase (Lyngaas, 2021). It is also essential to review how Colonial Pipeline managed its ransomware attack.

This was looked at in detail in an article by Nikolay Pankov in 2021. The author is a writer for Kaspersky antivirus solutions. He writes for the section known as Kaspersky daily, which addresses ransomware and other cyberattacks. In this article, he asked, should you contact authorities about ransomware? His conclusion and recommendation to all users, especially critical infrastructure owners, is to inform law enforcement properly. Informing law enforcement can significantly reduce the damage caused by hackers (Pankov, 2021).

He explained how contacting the authorities allowed for a quick response that ended with the Colonial pipeline going back online and even recouping some of its costs. The author is a strong proponent of cybersecurity. His position is to take action and mitigate all areas, but especially in the planning phase. Pankov's insight into cybersecurity provided valuable information about the colonial pipeline attack. This was emphasized on the technical exploit of the attack. He explained how the attack was executed and where the vulnerabilities were exploited in detail. In the case of the episode, ransomware's primary exposure was in the billing system and not so much the service networks. The author did go on to explain the mitigation and the response where the federal government quickly contacted ISP that owned the physical server and isolated it. Once this happened, the cybercriminals lost complete control of the colonial pipeline data and, therefore, their leverage(Pankov, 2021).

Discussion about the effectiveness of DarkSide's algorithm was general but sufficient to explain why it is impossible to access the data—once encrypted without the key. He also explained how Darkside works as a ransomware service model that provides the software to conduct the attack and even a service helpdesk with support. DarkSide is meant to be a strong advocate for malicious ativity (Pankov, 2021).

Lastly, the author went through several technical preplanning mitigation efforts that all critical infrastructure owners should adhere to. The list is extensive, discusses everything from remote desktops being more secure to backups being made readily accessible and offline, and using robust endpoint detection, response, and security. Although the article was short, it was informative and an excellent fact sheet for a technical perspective of the colonial pipeline ransomware attack. Since this article was more informative, it is difficult to find problems with its methodology or reasoning. However, it would have been good to mention more about the impact on Darkside by the government from a technical perspective. Did Darkside have secure software protection? What were Darkside vulnerabilities that allowed for counter-attacks?

Lessons learned were to contact the authorities if you are attacked. Getting the authorities involved quickly can lessen the impact of the attack. Also, use robust server security software to protect your data. All critical infrastructure owners should have mitigation plans in place. In an actual attack, particular attention should be given to defense strategies on any data that leaves the service with attention specific to outbound traffic. Backups should be kept offline so that a ransomware attack does not encrypt them. Use an end-to-end point security solution (Pankov, 2021).

To further examine how hackers exploited vulnerabilities, an article looked at what vulnerability the attackers used to access the colonial pipeline servers. The emphasis was on password security with some discussion about better managing passwords. There is some discussion about how malicious actors can obtain passwords and credential lists on the darknet. And finally, the article discusses how to disrupt the attack by reporting it to the authorities quickly and having a good recovery phase mitigation effort. The US government's role and quickly targeting Darkside was influential (*Colonial Pipeline Co. attack: What really happened*, 2021).

The author was a writer for Cyber Talk, a cybersecurity news and insight website geared for executives and businesses. The name of the author was not stated in the article. However, it was clear that they are proactive cybersecurity professionals employed by Cyber Talk. His key points were having suitable password security protocols and reporting cyberattacks quickly. Both of these actions are excellent mitigation against ransomware attacks (*Colonial Pipeline Co. attack: What really happened*, 2021).

The article provided an excellent summary of the ransomware attack on the Colonial pipeline. The primary focus of the article was how did the attackers get in? According to the report, the attackers used an old VPN account that had not been used in a while. Further research showed that the password used was also found with a more extensive trove of passwords on the dark web (*Colonial Pipeline Co. attack: What really happened*, 2021).

Limitations of this paper are as follows: The authors did not research and explain the cybersecurity already implemented for the Colonial pipeline. It is also curious, did the administrators not enforce password security question why were old accounts not disabled? A far more important question remains, how did the password become available on the dark web in the first place? This question remains unanswered as of the time of this writing.

The author then discusses the highlighted password security issue. Multi-factor authentication and other identity management methods are proposed. The article also highlights that large troves of passwords are dumped onto the dark web. Furthermore, the report states that these passwords are for sale and yield a 20 to 50% success rate on the targets that have been compromised. Further discussion on the use of multi-factor authentication should have been mentioned here. Multifactor the dictation would've prevented this hack even though the malicious actors had a valid password credential (*Colonial Pipeline Co. attack: What really happened*, 2021).

Lastly, the actions of Joe Biden issuing the state of emergency and targeted attack on Darkside's servers were listed as a successful mitigation effort. The discussion of the mitigation efforts by Joe Biden, such as empowering the FBI in the US Department of Justice to trace the cryptocurrency and reclaim the stolen bitcoin, was enlightening (*Colonial Pipeline Co. attack: What really happened*, 2021). However, more discussion on other successes in recovering bitcoin would have been good. Has this level of law enforcement action been taken before?

Lessons learned to pertain to password security. The primary protection against stolen passwords is to use two-factor authentication. A weakness or threat is that organizations or persons who do not employ two-factor authentication risk ransomware or other cybersecurity attacks. There is no barrier to the implementation of two-factor authentication. The only problem is that it is an additional step and thus an inconvenience for some. An article about the ransomware software developer DarkSide helps shed some light on these questions.

The study explains what ransomware is and how Darkside used ransomware as a service to conduct attacks against colonial pipelines. It also describes the federal pipeline security program and asserts that although pipeline infrastructure has federal regulations, the enforcement is weak. Pipeline infrastructure owners voluntarily follow the laws. The article also goes into Congress and addresses ransomware via federal agencies. Most of the argument is about who should have regulatory authority over pipeline security (Parfomak & Jaikaran, 2021).

The author's primary purpose is to inform the legislative debate about Congressional research. The role is technical as they help explain some technical concepts regarding ransomware. The introductory statement is that ransomware is malicious software used as ransomware as a service by criminal gangs and must be addressed by Congress and federal agencies. Another critical position is that the current regulatory authorities are insufficient to prevent future cybersecurity events. The agency with control over the federal pipeline should be clarified and possibly moved to the department of energy, the Department of transportation, or possibly even to FERC (Parfomak & Jaikaran, 2021).

The authors discuss the voluntary position of pipeline infrastructure operators. This is especially true in the area of cybersecurity. The TSA and pipeline owners have refused to make these positions mandatory because they believe that the voluntary following of regulations has been sufficient (Parfomak & Jaikaran, 2021).

Infrastructure owners voluntarily following the pipeline cybersecurity is disturbing to me. Because ransomware has already impacted our pipelines and fuel flow, not to mention other infrastructure impacts, we must move towards a mandatory cybersecurity regulation in critical infrastructure. However, the authors touched on this point. I emphasized it would have been good.

In the section where the authors discuss ransomware, they do not go into the vulnerabilities of the Colonial pipeline and how the password credentials were compromised, to begin with. It would've added substance to the discussion to explain to Congress and the public why the Colonial pipeline did not enforce cybersecurity protocols.

Where focuses on greater resource allocation to the TSA in its mission for pipeline security, Congress should look at increased funding for cybersecurity for our infrastructure and determine who is the most appropriate regulatory authority for pipeline security. Laws and regulations for pipeline security should be mandatory and not voluntary.

Lessons learned are that leaving voluntary regulations in place is insufficient to prevent a cybersecurity event. These voluntary regulations could also be considered a weakness in the pipeline infrastructure because they may cut corners in their cybersecurity efforts to maximize profits. It is important to remember that private entities own the pipelines, and therefore, profit is the driving motivator.

An opportunity that comes to light from the reading is the public, in general, should pass laws forcing pipeline Infrastructure owners to comply with mandatory regulations regarding cybersecurity. A barrier to this implementation could be political will, industry resistance due to cost, and other change deterrents. An unintended consequence may be an increase in fuel costs to customers. This is likely because of the cost of additional security protections for privately owned infrastructure. To understand government policies regarding cybersecurity, a look at the US Cybersecurity and Infrastructure Security Agency's guide on ransomware is necessary.

The guide has a profound explanation of ransomware. It uses best practices and recommendations from operational insight and multi-state information sharing and analysis. It is geared for information technology professionals and anyone responsible for developing cyber incident response policies and procedures or responding to cyber incident response. The guide states that the best prevention is prepared for ransomware attacks. The guide also claims that the ransomware vector is internet-facing vulnerabilities and misconfiguration of systems (*Ransomware guide*, 2020).

Lastly, the guide offers a ransomware response checklist. The checklist is comprehensive and includes detection and analysis, contact information and recovery, and post-is that activity procedures (*Ransomware guide*, 2020). The authors were anonymous cybersecurity experts within the department. The information was presented in a factual format with a bit of bias to the authors. The key to defeating ransomware is to follow the prevention best practices guidelines (*Ransomware guide*, 2020).

The guidelines present that the primary method for preventing ransomware is preparation. Preparation includes maintaining regular backups of all the operating systems configurations and virtual machines. It should also be efficient and quick to reinstall your backups (*Ransomware guide*, 2020).

The guide suggests maintaining cybersecurity is a response plan and the communications plan to show who is responsible for what and what notification procedures to follow in the event. It is essential to conduct regular vulnerability scanning to identify any vulnerabilities. CIS offers vulnerability scanning at no cost. It is also vital to regularly patch and maintain all systems, disabling or blocking outward-bound or outdated protocols. The authors discuss ransomware infection vectors fishing when malicious actors attempt to entice a user into loading a piece of malware. The authors also offer many resources for assistance (*Ransomware guide*, 2020).

The guide had all the technical information that might be wanted, along with multiple links for resources beyond the guide's scope. It was beneficial by providing the ransomware response checklist. It went through each of the steps that a cybersecurity expert would take in a ransomware attack (*Ransomware guide*, 2020).

The guide is very well written, with a significant amount of practical advice for organizations to secure their networks/systems. Organizational weaknesses or threats are that some companies may choose not to follow these guidelines and ignore the threat of ransomware. An opportunity is that before an organization becomes a victim of a ransomware attack, they can read this document and hopefully harden their systems and prepare themselves to defend against ransomware attacks. A barrier to implementation would be any costs or expenses resulting from implementing a more robust cybersecurity defense system (*Ransomware guide*, 2020). Colonial Pipeline did not follow many of these guidelines and thus, the breach exposed sensitive data.

Had the guidelines been followed, the impact of the ransomware would not have been as devastating as it turned out to be. According to Brian Fung (2021), personal information was also compromised. This went beyond the initial assessment that no other databases had been passed (Fung, 2021).

The article claims that cybercriminals also stole the personal information of close to 6000 Colonial pipeline employees. The stolen personal data consists of names, birth dates, social security numbers, drivers and military ID numbers, and emotional health information (Fung, 2021).

Fung is a reporter for CNN business. It reports the latest update of the Colonial pipeline ransomware attack. The author's key point is that private data was compromised, and the compromised persons were only recently informed. He provided a valuable update to the ongoing ransomware investigation. He described that the pipeline had only recently started sending letters notifying the impacted individuals of their data breach. Although, he mentions the content of the personal data that was compromised. He does not say what, if anything, the Colonial pipeline administration is going to do about it (Fung, 2021).

The pipeline should be held to account and offer to clean up for free any credits or privacy losses to their employees. The researcher should have mentioned the Colonial pipeline's liability due to their unsecured servers. The lesson learned is that entities that maintain team member information should maintain that information in encrypted form and unsecured servers.

There is an opportunity here to learn from the mistakes of the Colonial pipeline to take precautions to secure your servers and regain trust in the community. A barrier to implementation is the additional cost of securing database systems. Failure to do so can lead to compromised passwords access, as demonstrated by William Turton and Kartikay Mehrotra (2021).

The article identified that the hackers had access to the Colonial pipeline on April 29 via a compromised virtual private network. The password had also been found on the dark web. The author asserts that the password owner must've used the same password on a different account to be compromised in this fashion. Another assertion is that the password was not retrieved via a phishing attack (Turton & Mehrotra, 2021).

The author also explains that mediation in the response phase had taken place as security experts swept the network to figure out how the hackers attacked. At the time, the security experts determined that the hackers had not gone beyond the operational technology network, thus returning the pipeline to operational (Turton & Mehrotra, 2021).

This article is essential because there were two new pieces of information. The author asserts that the password owner must've used the password on a different account. This is important because it is common for people to reuse passwords. It is a high-security risk. To do this, though, It would have been stronger if the authors had given more evidence to support this hypothesis (Turton & Mehrotra, 2021).

Secondly, the author explains that during the mediation response phase, Colonial security experts had swept the network and determined that it was safe to return to operations. This is another area where it would have been good to have seen a more technical explanation of how the experts had concluded that the hackers had not gone beyond the operational technology network. The importance of this fact is emphasized by more recent articles that report that Colonial human resources databases had been hacked and that over 6000 employees' sensitive information had been compromised (Turton & Mehrotra, 2021).

Lessons learned in this article are that we must not reuse our passwords. It is best to use a password generator to use a different password for every need. Hackers know that users often reuse passwords to hack a more accessible system that reveals a password; they can then attempt to hack a more complex and secure system with the same password.

Organizational weaknesses are the lesson that you must patch your servers and enforce strict password policies. An opportunity from the research is to learn that your systems strengthen your passwords and have third-party auditing of your security systems. A Barrier to implementation again is cost and resistance to change by the administration. Offering bounties is one of the deterrents that the US government has to assist with the countermeasures to ransomware attacks. The following article by Scott Chipolina (2021) looks at bounties.

The bounties fall under the State Department's Rewards for Justice program (RFJ). The current rewards are offered for hackers acting under the control of a foreign government to attack US critical infrastructure. The program has been around since 1984 and has paid over $150 million for people who provided actionable intelligence that resulted in terrorists being placed behind bars. Recently, the Department of Justice raised ransomware to a similar level as terrorism. Currently, bounties are offered for hackers who explicitly use ransomware to access protected computer systems and damage infrastructure. The author points out that the US State Department is willing to pay out bounties in the form of bitcoin (Chipolina, 2021).

The authors provided some interesting information regarding the bounties for hackers. The article could be strengthened by discussing some of the bounties that have resulted in hackers being arrested. The report only mentioned terrorists brought to justice via the bounty program. The article does not mention if the bounties resulted in any actionable arrests for ransomware. Nor could any other paper that discussed bounties being successful against ransomware gangs be found.

The article also mentions moving to bitcoin as a form of payment but does not discuss bitcoin having been paid out yet for any other bounties. It does make sense that if bitcoin can stay anonymous, the informants will come forward to provide evidence. The Colonial attack was the first time Bit-coin had been offered.

Lessons an opportunity from the reading is bitcoin to encourage informants who desire to remain anonymous to come forward. The government taking this step will result in more actionable evidence against hackers. A barrier to implementation may be convincing Congress that it is in our best interest to allow informants to remain anonymous through the use of bitcoin. The reaction from Congress will not be known until the first bitcoin payment is paid out to an informant. An unintended consequence of implementing bitcoin payments might be hackers setting each other up and an innocent person's possible arrest and conviction.

**Conclusion and Future Areas of Study**

The May 2021 cybercriminal attack on the Colonial pipeline was a major attack on critical infrastructure. The mitigation planning phase was not done adequately by the Colonial pipeline. The organization failed to secure its databases and servers. By allowing an old VPN credential is to be active, they created an unnecessary vulnerability. While most ransomware attacks are made via phishing or social hacking, that was not the case with this attack. What is most disappointing is that this attack was preventable if the security team had just followed a strong cybersecurity planning guide (*Colonial Pipeline Co. attack: What really happened*, 2021; Fung, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

The US government provides ransomware guides and anti-ransomware software for free. On the government's websites. Cybersecurity experts have many resources to secure their systems (*Ransomware guide*, 2020). Therefore, Colonial Pipeline had no excuse for its failure to secure systems.

In October 2021, it was further disclosed that the hackers had compromised thousands of team members' sensitive data. This revelation contradicts Colonial pipelines cybersecurity personnel, who claimed that the initial breach did not reach sensitive data (Fung, 2021). This may lead to further litigation against Colonial Pipeline.

Colonial pipeline did a much better job during the response mitigation phase. The one thing they did right was contacting the government and report the breach. This quick decision resulted in minor damage and exposure and millions of dollars of bitcoin (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

The Biden administration reacted quickly by declaring a critical incident & freeing up federal funds, and authorizing rules and regulations to be temporarily halted to assist with fuel delivery. This rapid and vast response was solid action for communities and businesses. Additional action by the Justice Department also mitigated losses (*Colonial Pipeline Co. attack: What really happened*, 2021; *Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021).

The recovery mitigation phase was also much better. The government is much more proactive in conducting counter cyber operations using military assets if necessary. The US government is also more aggressive in pursuing cyber criminals by posting bounties paying out in bitcoin to apprehend cybercriminals. The strategy for handling hackers has shifted to a more proactive approach (Chipolina, 2021; Lyngaas, 2021; Menn & Bing, 2021).

As of this writing, the investigation into cybercriminals is ongoing. Future work on ransomware will have to include corrections to mitigation in the different phases for the Colonial pipeline. It will also be interesting to see if the $10 million bounty nets any cybersecurity criminals involved in this attack.

Furthermore, due to the prediction of an increase in ransomware and cyberattacks, it will be worth noting if Congress takes any action funding for cybersecurity and reorganizes the authority that pipeline regulations fall under. It will be challenging to conflict with the private sector (Pankov, 2021; *Ransomware guide*, 2020).

**Ransomware**

Ransomware is a piece of malware that has been written to infiltrate systems in particular servers and encrypt files. The malicious actors' target systems are likely to pay the ransom. The ultimate goal of cybercriminals is to rob victims of money. Typically bitcoin is the currency paid to decrypt the files (*Ransomware guide*, 2020).

Cybercriminals will often be careful in their targets to select companies, organizations that may pay and not report the attack to the authorities. However, in some cases, cybercriminals supported by foreign governments will use ransomware to attack critical infrastructure. An attack on any of the 16 critical infrastructure sectors vital to our nation would impact security, economic welfare, public health, and safety. The US government provides extensive information on detecting, preventing, and reporting ransomware via the CISA website. Here some resources assist with all phases of dealing with ransomware (*Ransomware guide*, 2020).

**DarkSide**

Darkside is a criminal group that writes ransomware software and offers it as ransomware as a service (Raas) and has been active since 2020. This group uses an extensive game hunting methodology that focuses on large organizations playing a significant ransom. Usually, companies with over $1 billion annual revenue are selected to be victims (Osborne, 2021).

This year alone (2021), DarkSide has committed 60 cases of ransomware extortion. These include only the ones that have been reported (Gallagher et al., 2021). Its latest version of ransomware is called Darkside 2.0. Affiliates who use this ransomware must pay Darkside 25% of any payments under $500,000 and 10% of any over $ 5 million (Osborne, 2021).

The primary vector used to penetrate systems is phishing. Phishing is a type of social hacking used to trick people into giving their credentials or clicking on a malicious link. In Colonial Pipeline, the credentials were purchased on the dark web. A previous employee had used the same password multiple times (Gallagher et al., 2021).

Blackmail is used to leverage organizations to pay the ransom to prevent sensitive data from being leaked online. Additionally, Darkside also has a web page where journalists can reach them directly. Darkside has tried to market itself as a type of Robin Hood. They have attempted to give some of the stolen money to charities. However, charities have rejected the stolen money (Osborne, 2021).

The attempt by Darkside to portray itself as a Robin Hood with a code of conduct has not been successful due to the attack on the Colonial pipeline. The colonial pipeline attack caused significant damage and suffering to the general population (Osborne, 2021). What is scary is that DarkSide will often spend months examining a victim's systems before initiating the ransom notice (Gallagher et al., 2021).

**Colonial Pipeline Mitigation Preparedness**

Colonial pipeline used password protections for access to their systems. They also had antivirus software and secured routers. Additionally, they voluntarily followed some of the TSA recommendations. Remember that pipeline security is only required to follow security guidelines set forth by the TSA voluntarily. The TSA offers substantial training and suggests that operators follow the national Institute of standards and technology cybersecurity framework to protect their systems (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

Colonial pipeline also had a plan for information that is quickly passed up to the administrators where decisions can be made in a cyber-attack. In the event of a problem, systems are taken offline through the authority of the senior administration (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021). The senior IT administrators did not follow or implement NIST cybersecurity recommendations (Turton & Mehrotra, 2021).

**Colonial Pipeline Mitigation Response Phase**

Entry to the network by hackers occurred on April 29th, 2021. The hackers announced themselves on May 7th, a little before 5 a.m. The shutdown process began almost immediately via the operations supervisor. The shutdown was complete by 6:10 a.m. Colonial pipeline reported the breach on May 7, 2021. Colonial's actions quickly brought the whole system down in just a little over an hour (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

This mitigation step put the gears in motion for the federal government to seize information on servers hosting Darkside ransomware, thus containing the attack. However, Colonial pipeline had previously paid $4.4 million in bitcoin to the hackers to decrypt their sensitive systems. Paying the ransom was a mitigation step for Colonial pipeline. Another mitigation step was to stop all pipeline operations on the eastern seaboard. This extended from New York to southern US states (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

Additionally, a physical inspection of the entire 29,000 miles of the pipeline was done. This was exhaustive and expensive work. Ground crews and helicopters were used for this task (Turton & Mehrotra, 2021).

Finally, the cybersecurity company Mandiant was brought in to assist with recovery efforts. Mandiant performed forensics on the systems to track the hacker's movements and determine when it was safe to resume operations. (*Colonial Pipeline Co. attack: What really happened*, 2021; Pankov, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021).

**Colonial Pipeline Mitigation Recovery Phase**

The US Department of Justice, with the assistance of the FBI, was able to recover 2.3 million in bitcoin due to the fast reporting by Colonial Pipeline (*Colonial Pipeline Co. attack: What really happened*, 2021; Parfomak & Jaikaran, 2021; Turton & Mehrotra, 2021). Fast reporting to the federal authorities remains a mitigation effort and sets an example for other entities to follow. The Biden Administration's decisive actions made all of the difference in this response.

Strict adherence to TSA pipeline security recommendations is being followed. The removal of legacy VPN applications is another mitigation effort. VPN usage is being overhauled, and more robust password requirements along with two-factor authentication will be a part of the mitigation plan (*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021; *Ransomware guide*, 2020).

Colonial technicians are also looking at other identity-management systems to limit vulnerability further. This includes following the zero-trust model. The model works on the concept of least privileged access and authentication protocols. This will ensure that only the correct users are granted access. Even then, it is restricted access to the hosts, ports, and other applications that may be needed (*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021; *Ransomware guide*, 2020).

Additionally, some internal review systems will be used to mitigate the risk of old VPN accounts. This system will audit the access permissions of each user and flag inappropriate access. This will prevent all the users or users with stolen credentials from moving about the system. It will also benefit from flagging any legacy software such as the legacy VPN so that IT personnel can deactivate any unused applications (*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021; *Ransomware guide*, 2020).

All critical infrastructure agencies should also use multi-factor authentication. This simple component would have secured Colonial pipeline from the ransomware attack. It has been estimated that only 40% of organizations currently use MFA (*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021).

MFA provides a multistep security approach to verify a person's identity trying to access information. Suppose the hacker tries to use a stolen login on a personal account. The MFA will stop the attempt because the hacker will not have the security token to complete the authentication step. MFA combined with employment verification, identity and access management systems, automatic provisioning, and de-provisioning user accounts create substantial barriers. The barriers created severely limit the threat vectors (*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021; *Ransomware guide*, 2020).

Lastly, Colonial hired Dragos Inc cybersecurity CEO Rob Lee as a consultant for cyber defenses (*Back to basics: A deeper look at the Colonial Pipeline hack*, 2021). It was good that Colonial recognized that it did not have the technical proficiency to secure its pipeline and thus turn to security professionals. However, It is worrisome that other critical infrastructure providers may not be following the complete recommendations provided by the NIST.

**Lessons learned**

After reading the relevant literature and studying this critical incident, all mitigation failures occurred in the planning phase. Many lessons can be learned from the missteps of the Colonial Pipeline. The most important lessons have to do with adequately securing critical infrastructure computer systems.

IT personnel must avoid complacency. Eternal vigilance must be the new motto of the IT cyberteam. Steps that must be followed to prevent additional breaches are listed below (Pankov, 2021; *Ransomware guide*, 2020).

* Disable all unnecessary ports when not in use, including remote desktop RDP and especially VPN.
* Robust security monitoring software must be in place to check incoming and outgoing packets on the internet.
* Password enforcement must be in place. Force users to create strong passwords and change them periodically. This one step would have prevented the Colonial breach.
* Systems should be patched weekly.
* Back up all databases and systems regularly and store backups in an air-gapped environment. In a breach, the offline backups will be unaffected and thus make restoration easier.
* Threat intelligence must be a part of the daily reading for IT professionals. It is the only way to be up to date on the latest attack vectors, tactics, techniques, etc.
* Install a robust endpoint detection response security system. The system should also protect against abnormal behavior to do rollbacks if malicious changes have been detected to restore the system.
* Training must be completed from a security mindset. Especially true for IT in charge of critical infrastructure.
* In the event of a breach, contact the authorities immediately.
* Have a good incident response plan that has detailed instructions on what to do in the event of a breach. Response, notification plan, along checklist will be invaluable during an attack (*Ransomware guide*, 2020).
* The principle of least privileges for all systems and services must be used. This principle restricts users to the authority required to do their job and no higher (*Ransomware guide*, 2020).
* Permanently remove old or unnecessary accounts. Colonial IT failed in this step.
* Audit user accounts (*Ransomware guide*, 2020).
* Make sure good computer logs are kept. Analysis of logs is how events are analyzed (*Ransomware guide*, 2020).

**Conclusion**

If the above-listed security steps had been followed, the Colonial Pipeline breach would not have happened. From experience working in the IT field over the last twenty years, IT personnel laziness and complacency are the main threats to system security. When nothing happens year after year, it is easy to fall into this trap.

As noted, Darkside acquired a former employee's user credentials from the Darkweb and then accessed Colonial's systems via a legacy VPN connection. Had Colonial IT removed legacy systems, the breach would not have happened. Colonial IT needed to disable old user accounts. Also, if Colonial had endpoint monitoring software, the breach would not have happened. This was a significant and easily preventable IT failure. The head of IT along with the IT department should be fired.

The unfortunate part about the Colonial IT incident is that most of the security steps listed above do not cost anything to implement. They are necessary procedural tasks that are expected from IT. Most IT departments implement several of these security measures.

**Colonial Pipeline Ransomware Cyber-Attack Stakeholders Map**

The following is the stakeholder map that provides a visual for viewing the different entities and relationships. Many different stakeholders interacted to impact all three areas of the mitigation responses. The four quadrants and their respective entities were discussed in depth in the stakeholders' section of this paper on page 9.

Graphical user interface, diagram

Description automatically generated

References

*Back to basics: A deeper look at the Colonial Pipeline hack*. (2021). Government technology. Retrieved December 3 from <https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack>

Chipolina, S. (2021, August 16th, 2021). *US Government to offer dark web informants bounties in crypto*. Decrypt. Retrieved November 21 from <https://decrypt.co/78609/us-government-offer-dark-web-informants-bounties-crypto>

*Colonial Pipeline Co. attack: What really happened*. (2021). cybertalk.org. Retrieved November 4 from <https://www.cybertalk.org/2021/06/09/colonial-pipeline-co-attack-what-really-happened/>

*Fact Sheet: The Biden-Harris administration has launched an all-of-government effort to address Colonial Pipeline incident*. (2021). The White House. Retrieved November 5 from <https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/11/fact-sheet-the-biden-harris-administration-has-launched-an-all-of-government-effort-to-address-colonial-pipeline-incident/>

Fung, B. (2021). *Colonial Pipeline says ransomware attack also led to personal information being stolen*. CNN. Retrieved November 21 from <https://www.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html>

Gallagher, S., Loman, M., Mackenzie, P., & Pollat, Y. (2021). *A defender's view inside a DarkSide ransomware attack*. Sophos News. Retrieved December 2 from <https://news.sophos.com/en-us/2021/05/11/a-defenders-view-inside-a-darkside-ransomware-attack/>

Johnson, R. (2015). *Security policies and implementation issues* (2nd ed.). Jones & Bartlett Learning.

Lyngaas, S. (2021). *State Department offers $10M for information on Colonial Pipeline hackers*. CNN. Retrieved November 5 from <https://www.cnn.com/2021/11/04/politics/colonial-pipeline-ransomware-hacking-reward-state-department/index.html>

Menn, J., & Bing, C. (2021, Friday, October 22nd). Exclusive: Governments turn tables on ransomware gang revil by pushing it offline -sources. *The Star*. <https://www.thestar.com.my/tech/tech-news/2021/10/22/exclusive-governments-turn-tables-on-ransomware-gang-revil-by-pushing-it-offline--sources>

*Microsoft digital defense report*. (2021). Microsoft. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi>

Osborne, C. (2021). *DarkSide explained: The ransomware group responsible for Colonial Pipeline attack*. Zero Day. Retrieved December 2 from <https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained/>

Pankov, N. (2021). *How Colonial Pipeline managed its ransomware attack: Should you contact authorities about ransomware?* Kaspersky. Retrieved November 4 from <https://www.kaspersky.com/blog/pipeline-ransomware-mitigation/39907/>

Parfomak, P. W., & Jaikaran, C. (2021). *Colonial Pipeline: The DarkSide strikes*. Congressional Research Service. Retrieved November 4 from <https://crsreports.congress.gov/product/pdf/IN/IN11667>

*Ransomware guide*. (2020). Multi-State Information Sharing & Analysis Center Retrieved from <https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf>

Turton, W., & Mehrotra, K. (2021). *Hackers breached Colonial Pipeline using compromised password*. Bloomberg. Retrieved November 21 from <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>