3/6/2022

# The Colonial Pipeline Ransomware Attack

## Cyber Incident Management


**Team 3:**

- Dennis Tarus- 005
- Denis Kiplangat- 004
- Okello Onyando- 016
- Joseph Waigwa- 012
- Mwende Mohammed -015

# Executive Summary

The use of the internet and digital systems by governments and organizations necessitates incident management processes or plans to be in place given the negative impacts cyber-related attacks have, such as paralyzing the daily activities of an institution, thus a threat to business continuity. Ransomware attacks continue to be one of the biggest cybersecurity threats to both private and government institutions all over the world. Mitigating such cyber threats, companies always try to come up with an incident response plan to avoid, reduce, transfer or reduce the risk while also complying with the laws put in place by the state. In case of an attack, various standards to recover from cyber incidents are put in place by different entities.

In this paper, the National Institute of Standards and Technology (NIST) incident response framework is used to assess the response plan of Colonial Pipeline Company which suffered a ransomware attack. The company, as a critical infrastructure, is the United States' largest pipeline system for refined oil products. The framework highlights key steps to undertake in the anticipation of a potential attack which are preparation, detection and analysis, containment, eradication and recovery, and post-incident activities that involve lessons learnt from the event. The company was said not to have a well-defined incident management strategy since Cybersecurity and Infrastructure Security Agency (CISA) had warned of the attack in 2020. Threat actors called “Dark Side” believed to be operating from Russia targeted the company on 29th April, 2021. The attack was possible through the use of credentials of a dormant Virtual Private Network account which still had access to the company systems and lacked security measures such as the use of multi-factor authentication and good industry practice of disabling or deleting inactive user accounts.

To mitigate the incident, both short term and long-term measures were put in place to reduce the impact of the attack. All critical operation systems were shut down for six days to pave way for a thorough analysis to determine the depth of the attack. Due to the nature of the attack where systems were held “hostage” and exfiltration of nearly 100 gigabytes of data, the company did not have much to do but to pay $4.4 million as the ransom. In addition, Joe Biden, the president of the USA declared a state of emergency to regulate the sale of fuel in the country to reduce the impact of the attacks on fuel consumers. To mitigate such compromise, organizations should adopt relevant cybersecurity policies and regulations that put in place measures of ensuring dormant accounts are disabled as well as auditing of the company systems. Furthermore, companies should hire adequately skilled cybersecurity personnel and use multi-factor authentication when securing user accounts. Governments and organizations are also encouraged to adopt and effectively implement incident response plans in order to prevent and reduce the impacts brought by cyber incidents.

# Table of Contents



# Table of Figures

# The Colonial Pipeline Ransomware Attack

## Introduction

A cyber incident is a violation of computer security policies, acceptable use policies, or standard computer practices. A cyber incident response plan gives the incident response team basic directions on what to do immediately following a cybersecurity occurrence. This enables an organization to respond to incidents systematically taking appropriate actions in order to minimize loss or theft of information and disruption of services. The information gained during incident handling can be used to prepare for handling of future incidents and provide stronger protection for systems and data.

In May 2021, the Colonial Pipeline was the target of a ransomware attack. It infected the pipeline's digital systems, resulting to being taken offline for several days affecting consumers and airlines along the East Coast. Because the pipeline transports oil from refineries to industry markets, the intrusion was declared a national security threat. President Joe Biden responded by declaring a state of emergency.

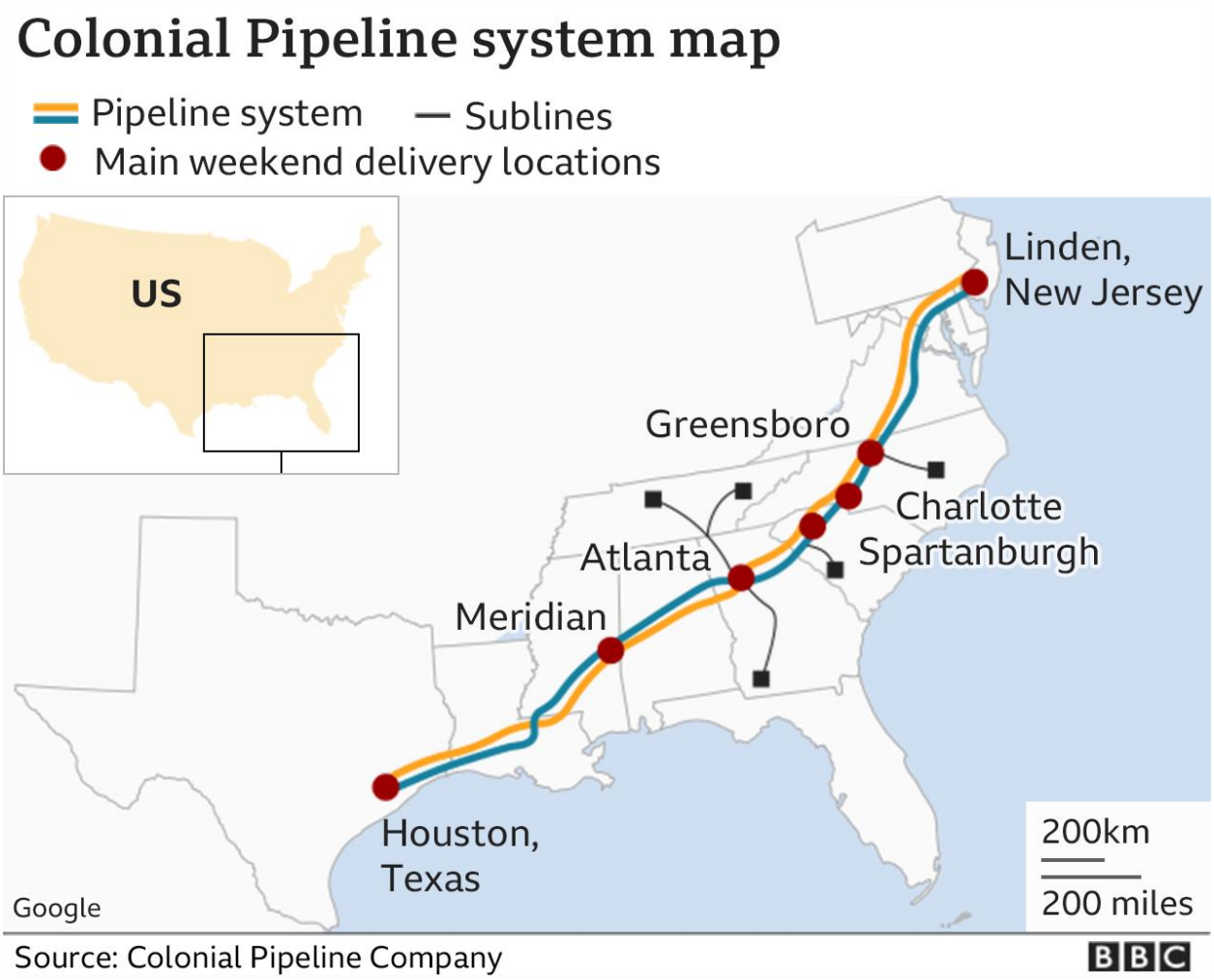


*Figure 1 Colonial Pipeline System Map*

The Colonial Pipeline began in 1962 to help move oil from the Gulf of Mexico to the East Coast states and is one of the largest and most vital oil pipelines in the U.S. It comprises more than 5,500 miles of pipeline running from Texas all the way up through New Jersey, supplying nearly half of fuel for the East Coast. It delivers refined oil for gasoline, jet fuel and home heating oil. To handle this incident, the company followed the various steps as in the NIST cybersecurity incident response plan. This document gives a critical evaluation on how effectively the company followed the steps from preparation, detection and analysis, containment, eradication and recovery to post-incident activity. It also gives various recommendations on how the incident could have been handled better to minimize the impact of the ransomware to the Colonial Pipeline.

# Critical Evaluation

## I. Preparation

In May 7, 2021, the Colonial Pipeline Company proactively shut down its pipeline system in response to a ransomware attack. The operations resumed on May 13, 2021.

**What the Company Did**

The following actions were taken by the company in response to the ransomware attack:

- **Communication**

The company posted a statement on their website about the ransomware attack. A third-party cybersecurity firm was engaged to perform the investigations. Law enforcement and other federal agencies were also contacted. In the statement, the company outlined their primary focus; safe and efficient restoration of services and resumption of normal operations.[1] In addition, being a private company, Colonial Pipeline worked together with the government to disrupt the attack, and pledged to share the vulnerabilities findings with the government, and other companies so as to better prepare for and prevent further attacks of the same nature.[2]

- **Incident mitigation**

According to the testimony given by the Colonial Pipeline CEO in a hearing before the Senate Homeland Security and Government Affairs, the company did not have a plan in place on how to handle a ransom demand from the cybercriminals who held their systems. He however, stated that the company had an emergency response plan: see the threat, contain the threat, remediate the threat, and restore.[3] In response to the attack, the company first shut down its pipeline system to prevent the attack from spreading to the operational technology environment, then investigations started after. The investigation aimed at determining if data was breached, and the leverage the company had to reduce the ransom demand.

- **Risk assessment**

Assets – The IT network was impacted by the ransomware attack, not the operational technology. The company then shut down pipeline operations temporarily to ensure that infection would not spread to operational technology environment.[4]

1 Segal, E., 2021. 7 Crisis Management Lessons From Colonial Pipeline's Response To Cyber Attack. [online] Forbes. https://www.forbes.com/sites/edwardsegal/2021/05/08/colonial-pipeline-cyber-attack-is-providing-crisis-management-lessons-in-real-time/?sh=43e53cea3d82

2 Cohen, Z. and Sands, G., 2021. Four key takeaways on the US government response to the pipeline ransomware attack. [online] CNN.https://edition.cnn.com/2021/05/11/politics/colonial-pipeline-cyber-hearing-senate-homeland-security-committee/index.html

3 Riley, T., 2021. Colonial Pipeline CEO says company didn't have plan for potential ransomware attack. [online] CYBERSCOOP. Available at: <https://www.cyberscoop.com/colonial-pipeline-ransomware-senate-hack/> [Accessed 1 June 2022].

4Cyber.nj.gov. 2021. Colonial Pipeline Incident: Ransomware Impacts and Mitigation Strategies. [online] https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/colonial-pipeline-incident-ransomware-impacts-and-mitigation-strategies

Risks - The company lost substantial revenue due to several days of shutdown, and ransom payment. Besides, the pipeline is a critical infrastructure and the attack had impact to the public as well. In addition, if the attack spread to the operational technology environment, it could have been catastrophic.

Monitoring/Response activities - Heavy investment for new infrastructure; the company did not have trust in rebuilding on the same infected network.[5]

- **Securing infrastructure, applications and users**

The company failed to prepare explicitly for a ransomware attack, despite being warned by Homeland Security Department's Cybersecurity and Infrastructure Security Agency in February 2020 about the risk of ransomware attacks against the pipeline industry.[6]

**What could have been done better?**

In regards to the ransomware attack, the company responded fairly to the attack. However, there are areas which could have been done better. These include:

- The company could have paid close attention the potential attack warning issued to them by the Homeland Security Department's Cybersecurity and Infrastructure Security Agency to harden their systems and prepare well for any attacks.
- The company did not know how to handle the ransom demands, they took long to pay the ransom, thereby loosing on the operations before later paying the ransom. In this case, the company could have paid the ransom earlier if they knew very well that they did not know how to handle the ransomware incident.

To prevent or better handle such attacks in future, the following actions are recommended:

- Ensure firewalls are enabled, properly configured, and monitored.
- Conduct user cyber threat awareness training and phishing simulations.
- Have a comprehensive data backup plan in place including multiple offline backup copies kept in a secure location.
- Monitor for unusual outbound data transfers that could indicate the data exfiltration leading to ransomware attack.

5 Segal, E., 2021. 7 Crisis Management Lessons from Colonial Pipeline's Response To Cyber Attack. [online] Forbes. https://www.forbes.com/sites/edwardsegal/2021/05/08/colonial-pipeline-cyber-attack-is-providing-crisis-management-lessons-in-real-time/?sh=43e53cea3d82

6 Riley, T., 2021. Colonial Pipeline CEO says company didn't have plan for potential ransomware attack. [online] CYBERSCOOP.https://www.cyberscoop.com/colonial-pipeline-ransomware-senate-hack/

- Identify the company's assets and put a plan in place to protect these assets.

## II. Detection and Analysis

Detection involves obtaining information from IT systems, security tools, publicly available information, and people both inside and outside the enterprise, as well as recognizing precursors (indications that an incident may occur in the future) and indicators (data showing that an attack has happened or is happening now). On 6th May, 2021, Info Servers used in the Supervisory Control and Data Acquisition (SCADA) stack were infiltrated and over 100 gigabytes of data were confiscated from Colonial Pipeline's systems in just under two hours[7]. Before the ransomware could infect downstream systems, security personnel detected the threat and took them down to prevent further damage.

Analysis involves establishing a baseline or normal activity for the afflicted systems, correlating relevant occurrences, and determining whether or not they vary from normal behavior. On 9th May, 2021, DarkSide was suspected of being engaged in the attack. The impact of the attack on the nation's energy supply was monitored by the Department of Energy[8]. Upon learning of the issue, a third-party cybersecurity firm (Mandiant) was engaged, and they launched an investigation into the nature and scope of the ransomware. The company also contacted law enforcement and other federal agencies. DarkSide was able to access and seize control of Colonial Pipeline's network by simply logging in to a "legacy VPN" that was still operating within the system using a single leaked password and user name combination according to a report by CISA and the Federal Bureau of Investigation (FBI)[9]. Because the VPN did not need multi-factor authorization, DarkSide was able to paralyze and entirely shut down the company's operations after entering the proper credentials. The company disclosed in a statement that only its corporate IT network was impacted, not their Operational Technology (OT) network[10].

The Colonial Pipeline would have used techniques to detect and stop this attack at the earliest stages of the kill chain before any damage or encryption was done. An example of a technique is the Endpoint Privilege Management solution. Ransomware is rendered ineffective by robust EPM systems that stop any process or program trying operations that are prohibited – such as encryption – regardless of the user's privilege level[11]. The company could have also monitored for suspicious

[7] Virsec.com. 2022. Virsec Analysis of the Colonial Pipeline Attack. [online] https://www.virsec.com/blog/virsec-analysis-of-the-colonial-pipeline-attack
[8] Picirrilli, C., 2022. How the Colonial Pipeline attack occurred. [online] wtw.https://www.wtwco.com/en-US/Insights/2021/05/how-the-colonial-pipeline-attack-occurred.
[9] Federal Bureau of Investigation. 2021. FBI Statement on Compromise of Colonial Pipeline Networks | Federal Bureau of Investigation. [online] Available at: https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks
[10] Cyber.nj.gov. 2021. Colonial Pipeline Incident: Ransomware Impacts and Mitigation Strategies. [online] https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/colonial-pipeline-incident-ransomware-impacts-and-mitigation-strategies
[11] Cyber.nj.gov. 2021. Colonial Pipeline Incident: Ransomware Impacts and Mitigation Strategies. [online] Available at: <https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/colonial-pipeline-incident-ransomware-impacts-and-mitigation-strategies> [Accessed 3 June 2022].

outbound data transfers that could indicate the exfiltration of data that may precede a ransomware infection. It is recommendable for the company to perform threat hunting which is a methodology of identifying ransomware, so the threat can be contained before encryption begins. Through this technique, analysts can find and analyze all unique or suspicious persistence mechanisms on a device.

## III. Recovery, Eradication and Containment

Short-term and long-term mitigation strategies to the attack were taken to ensure that the threat did not escalate further. According to Colonial Pipeline Chief Executive officer Mr. Joseph Blount, just before 0500hrs of May 7, 2021, a Colonial control room staffer noticed a ransom note demanding bitcoins. The employee alerted an operations supervisor, who began the procedure of shutting off the pipeline right away because they had no notion who was attacking them or why[12]. Colonial began an extensive assessment of the pipeline soon after the incident, tracking 29,000 kilometers on the ground and in the air to search for visible damage. The pipeline was not harmed. The password used to hack was also deactivated. In addition, security teams analyzed the network and also installed new detection and alerting tools. The company also paid a ransom to the attackers of $4.4 million after which a tool was provided to unlock the compromised systems. Two security experts were also employed to help in matters of cyber security. Joe Biden, the President of the United States, declared a state of emergency on 9th May, 2021 to regulate use of fuel consumption. The president also issued an Executive Order 14028 on the 12th May, 2021, tightening software security standards for government purchases, improving information sharing and training, establishing a Cyber Safety Review Board, and improving incident response[13]. A cybersecurity task group was also formed by the US Department of Justice in order to enhance prosecutions.

It is notable that taking backups and continuous patching of software is one of the best preventive measures against a ransomware attack[14]. In addition, it is advisable to develop plans and policies that will ensure that inactive user accounts and passwords are removed[15].

Threats that emanate from cyber incidents have the potential of threatening the business continuity of an organization. As for the case study on the colonial pipeline ransomware attack, day to day operations of the company were affected and the company had to immediately shut down its systems to avoid further spread of the attack for a period of 6 days resulting in cases of fuel shortages. To be able to bring the systems online and resume normal operations, recovery measures needed to be applied to manage the incident.

[12] Turton, W. and Mehrotra, K. (2021). Hackers Breached Colonial Pipeline Using Compromised Password. New York: Bloomberg
[13] Wikipedia, (2022). Colonial Pipeline ransomware attack.
[14] Guidance, (2021). Mitigating malware and ransomware attacks.
[15] CIS, (2022). 7 Steps to Help Prevent & Limit the Impact of Ransomware.

Recovery as part of incident management involves the restoration of systems to their normal operational state and in other scenarios mitigation of weaknesses or vulnerabilities within a system to prevent future occurrences of related system attacks[16]. In order to resume operations, colonial pipeline hired cybersecurity experts who were able to traverse the network and systems of the company to ensure there existed no traces of the attackers and as part of the process the incident responders deployed detection tools to alert on other possible breaches after the attack. With all the precautionary measures taken into account and ensuring no attackers were still in the network, the digital systems of the company were then restored to normalcy.

## IV. Post-Incident Review

The post incident activity step is a crucial step in any incident management process to learn and improve in planning for other incidents. An incident management team or the security team are required to hold a meeting with every stakeholder within an organization affected by the incident and can elect to do it periodically to improve the security handling procedures and processes. The meeting aims to review all the questions arising from the incident, effectiveness of the response and where can be improved. There are various areas identified within the postmortem to be covered such as timeline of events, management of the incident, staff involved, and lessons learnt.[17]

Charles Carmakal from Mandiant, stated that hackers were able to gain entry into the company's networks through a dormant virtual private network account. The attackers got hold of the password that was later discovered among other leaked passwords from the dark web demonstrating importance of thorough threat intelligence. Another discovery made was on failure to implement multifactor authentication on the compromised account. Lack of proper access controls, audit and password hygiene through use of different passwords led to success of the attack. Mandiant traced attackers' movements within the network to ascertain the severity of the attack and found out the critical operational systems controlling flow of gasoline were not affected but the informational technology network indicated previous hacker footprints. The company engaged industrial control systems cybersecurity experts, Rob Lee and John Strand to bolster their cyber defenses and urged the government to go after the attackers.[18]

Darkside was confirmed as the hackers responsible for the attack by the FBI. The hacker group offers services for example ransomware as a service. The FBI affirmed its support on the investigation

[16] Cichonski, P., Millar, T., Grance, T. and Scarfone, K., 2012. *Computer Security Incident Handling Guide*. [online] NIST. https://www.nist.gov/publications/computer-security-incident-handling-guide

[17] NIST. (2012). *SP 800-61 rev. 2, computer security incident handling guide*. NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[18] Turton, W. (2021, June 4). Bloomberg. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

as the attackers proclaimed on their website that their intention was to make money and not to cause any disruptions in the society. The incident caused a rise in fuel price to $2.967; six cents rise per gallon. There were fears of continued rise if the shutdown prolonged.[19] Proactive approach to cybersecurity is key through investment in security, frequent audits and partnerships with government and partners to deter threats.

**Recommendations**

- Thorough checks on implemented access controls effectiveness and where to improve. The access to informational technology network and almost breach of critical operations network would have been severe. Isolation and segmentation of data systems and pipelines need be separated to reduce extent of attacker's movement.[20]
- Strong and different passwords across accounts combined with multifactor authentication is important in protection of accounts and limiting access to only account holders.[21]
- Frequent risk assessments to determine the exposure of the company should be implemented to reduce exposed services and attack surface.

# Conclusion

Following the ransomware attack on the Colonial Pipeline, business and government set out to identify measures to minimize or prevent similar attacks in the future. The Biden Administration issued an executive order in May 2021 urging US government entities to take a range of proactive cybersecurity measures[22]. The use of a Software Bill of Materials (SBOM) is one of the actions recommended by the order. SBOMs allow organizations to manage dependencies, discover security concerns early and remediate them, and ensure that they are achieving the security posture standards. While there is no "one way" to construct a plan, there are best practices for creating and evaluating an ideal incident response plan, such as those outlined in the NIST Incident Response framework, that will help organizations be more resilient in the event of a cyberattack. With a successful incident response program, damage can be mitigated or avoided altogether.

[19] Russon, M. (2021, May 10). US passes emergency waiver over fuel pipeline cyber-attack. BBC News. https://www.bbc.com/news/business-57050690
[20] Sanger, D. (2021, May 16). Pipeline attack yields urgent lessons about U.S. cybersecurity. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html
[21] https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/
[22] Cichonski, P., Millar, T., Grance, T. and Scarfone, K., 2012. *Computer Security Incident Handling Guide*. [online] NIST. https://www.nist.gov/publications/computer-security-incident-handling-guide

# References

Cichonski, P., Millar, T., Grance, T. and Scarfone, K., 2012. Computer Security Incident Handling Guide. [online] NIST. https://www.nist.gov/publications/computer-security-incident-handling-guide

Cichonski, P., Millar, T., Grance, T. and Scarfone, K., 2012. Computer Security Incident Handling Guide. [online] NIST. https://www.nist.gov/publications/computer-security-incident-handling-guide

Cohen, Z. and Sands, G., 2021. Four key takeaways on the US government response to the pipeline ransomware attack. [online] CNN.https://edition.cnn.com/2021/05/11/politics/colonial-pipeline-cyber-hearing-senate-homeland-security-committee/index.html

Cyber.nj.gov. 2021. Colonial Pipeline Incident: Ransomware Impacts and Mitigation Strategies. [online] https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/colonial-pipeline-incident-ransomware-impacts-and-mitigation-strategies

Cyber.nj.gov. 2021. Colonial Pipeline Incident: Ransomware Impacts and Mitigation Strategies. [online] https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/colonial-pipeline-incident-ransomware-impacts-and-mitigation-strategies

Federal Bureau of Investigation. 2021. FBI Statement on Compromise of Colonial Pipeline Networks | Federal Bureau of Investigation. [online] Available at: https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks

NIST. (2012). SP 800-61 rev. 2, computer security incident handling guide. NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Picirrilli, C., 2022. How the Colonial Pipeline attack occurred. [online] wtw.https://www.wtwco.com/en-US/Insights/2021/05/how-the-colonial-pipeline-attack-occurred.

Riley, T., 2021. Colonial Pipeline CEO says company didn't have plan for potential ransomware attack. [online] CYBERSCOOP. Available at: <https://www.cyberscoop.com/colonial-pipeline-ransomware-senate-hack/> [Accessed 1 June 2022].

Riley, T., 2021. Colonial Pipeline CEO says company didn't have plan for potential ransomware attack. [online] CYBERSCOOP.https://www.cyberscoop.com/colonial-pipeline-ransomware-senate-hack/

Russon, M. (2021, May 10). US passes emergency waiver over fuel pipeline cyber-attack. BBC News. https://www.bbc.com/news/business-57050690

Sanger, D. (2021, May 16). Pipeline attack yields urgent lessons about U.S. cybersecurity. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

Segal, E., 2021. 7 Crisis Management Lessons From Colonial Pipeline's Response To Cyber Attack. [online] Forbes. https://www.forbes.com/sites/edwardsegal/2021/05/08/colonial-pipeline-cyber-attack-is-providing-crisis-management-lessons-in-real-time/?sh=43e53cea3d82

Segal, E., 2021. 7 Crisis Management Lessons From Colonial Pipeline's Response To Cyber Attack. [online] Forbes. https://www.forbes.com/sites/edwardsegal/2021/05/08/colonial-pipeline-cyber-attack-is-providing-crisis-management-lessons-in-real-time/?sh=43e53cea3d82

Turton, W. (2021, June 4). Bloomberg. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Turton, W. and Mehrotra, K. (2021). Hackers Breached Colonial Pipeline Using Compromised Password. New York: Bloomberg

Virsec.com. 2022. Virsec Analysis of the Colonial Pipeline Attack. [online] https://www.virsec.com/blog/virsec-analysis-of-the-colonial-pipeline-attack