TITLE PAGE

Student First and Last Name: Dawda Wally

Student ID: R2404D17931625

Date of Submission: 04th August 2024

Assignment Name: uel-cn-7014-assignment-1.

Module Name and Code: UEL-CN-7014-64357 Security Management (64357)

Table of Contents

1. Part 1A - Cyber Attacks

1.1 Introduction

The developments in technology within the 21st century have made life easier and the running of organizations and society's societal frameworks convenient; nevertheless, this has rendered important technical and computer systems susceptible to cyber threats. A key example of such threats is the attack that occurred on the Colonial Pipeline in May 2021.

Colonial Pipeline Company owns the largest pipeline through which fuel is transported in the United States; this pipeline has a length of 5,550 miles stretching from Texas to New Jersey. The cyber attack on the company forced it to close its pipeline which led to scarcity and a spike in the price of fuel in the eastern part of the United States. This disruption highlighted glaring threats in the cybersecurity of the infrastructural sectors comprising critical assets (CISA, 2021; Greenberg, 2021).

The type of attack on Colonial Pipeline was typically carried out using software that locks the target's files and/or data and then extorts a specific sum of money for the decryption of the files (Bosworth, Kabay and Whyne, 2014). It is also important to note that the ramifications were not limited to monetary damages and the case raised questions about the matters of national security and the impact that the participation of governments and external security agencies could have during and after such incidents (Boulton, 2021).

The attack has presented a need for good cybersecurity systems in organizations, and the need to be prepared to handle such an incident. Colonial Pipeline Company's management caved into the demand of the hackers and they paid the amount which was estimated to be around $4. 4 million—the ransom payment is an example of a contentious business decision that demonstrates that operational disruption and business losses are not the only effects that have to be considered (Buchanan, 2011). The subsequent FBI's action of recovering some of the ransom shows the paradoxical quality of the policing function in addressing cybercrime, namely the capacity and limitations (Greenberg, 2021).

This report considers the attack characteristics of Colonial Pieline, the involved actors, harnessed weaknesses, and actions taken in response to mitigate risks. The report also builds on the impact of this specific incident on the cybersecurity of critical infrastructure.

1.2 Incident Overview

The Colonial Pipeline system was shut down on May 7, 2021, as a result of an attack by the ransomware hacker group called DarkSide. The attack targeted the company's IT infrastructure and compromised it. They penetrated the pipeline's management systems and extorted the decryption code from the company's system. Subsequently, to prevent the malware from spreading further to the company's other operational control systems, Colonial Pipeline closed its pipeline (CISA, 2021).

The degree of seriousness of the attack was further ascribed to the ramifications in the short-run as well as the long-run impacts on security and the economy of the nation. Fuel stations attracted people by their scarcity, people had to stand in queues for fuel and at the same time there was also an increment in fuel prices. It also paved the way for debates on the preparedness of owners and operators of critical infrastructures against such highly sophisticated threat actors (Boulton, 2021).

1.3 Incident Analysis

1.3.1 Who Was Affected

The impacts of the cyber attack against the Colonial Pipeline were rather subjective and considered the different facets of the organization's operations. Below are some of the stakeholders that were affected by the cyber-attack:

1.3.2 Colonial Pipeline Company: Colonial Pipeline whose pipeline was attacked, lost operation, more money and its reputation to the attackers. This event was a clear demonstration

of the magnitude of the corruption issue within some protective structures of the firm because the organisation stopped the use of the pipeline after the leakage.

1.3.3 Consumers and Businesses: Some of the issues that were realized as a result of the shutdown are the fuel crisis that has affected millions of people as well as several other institutions that rely on its consumption.

1.3.4 Government and Regulatory Bodies: This happened mainly to trigger an intervention of the federal agencies comprising the Cybersecurity and Infrastructure Security Agency (CISA) together with the Federal Bureau of Investigation (FBI).

1.4 Kind and Category of Cyber Attacks

The attack on Colonial Pipe was of the ransomware kind which is a kind of malware that invades a user's computer, locks their files, and demands a certain amount of money for the files to be decrypted. The members of the DarkSide cybercrime community broke into the business computer system of Colonial Pipeline using ransomware(CISA, 2021).

1.5 The Severity of the Cyber Attack

The impact of the attack was intense and had severe effects on the economic and operating aspects of the company. This affected the supply of fuel across the eastern part of the United States hence causing fuel scarcities, high prices, and a rush for fuel. The economic effects were an increase in transportation costs, effects on businesses that use fuel, and a domino effect on the economy (Boulton, 2021).

1.6 Threat Actors and The Reasons Why They Acted The Way They Did

The group responsible for the cyberattack is called DarkSide and is considered one of the most professional cybercriminal groups specialising in ransomware attacks. The group's objectives seemed profit-oriented as it demanded a ransom to decrypt the encrypted files. However, the case also provoked concerns about the possible state actors' influence or geopolitical context since the affected infrastructure was crucial (Greenberg, 2021).

1.7 Some of the common Indicators of Compromise (IOCs)

Some of the attributes of Indicators of Compromise (IOCs) associated with the Colonial Pipeline attack were C2 Server IP Addresses, executable files, weak networks etc. Some of the IOCs are listed and discussed below

Malicious IP Addresses and Domains: These are used by the attackers in command and control of the systems and as a means of management of the release of ransomware.

Ransomware Executable Files: These files were recovered in the specified penetrated computers and their function was to encrypt information.

Unusual Network Activity: The temporal trends of data encryption and communicating with the resources outside the organization as a characteristic of ransomware attacks have been recognized in the network traffic (CISA, 2021).

1.8 Elements of Security Compromised (C.I.A. Triad)

The Colonial Pipeline ransomware attack compromised critical elements of the C.I. A. triad in the following ways:

1.8.1 Confidentiality

Confidentiality looks at the ability a business or an organization has to avert the passage of information to any undesirable or unauthorized person (Bosworth, Kabay and Whyne, 2014). In the case of the Colonial Pipeline attack, confidentiality was compromised in multiple ways.

1. **Data Encryption**: This attack involved successfully encrypting the company's sensitive files. These criminals also see it wise to encrypt the data in a way that it nearly impossible for legitimate users of the data to access it without the consent of the criminals (Boulton, 2021).
2. **Risk of Data Exfiltration**: This means that the criminals illicitly acquire sensitive information and then encrypt it (ISO/IEC, 2013; Greenberg, 2021).

1.8.2 Integrity

Integrity here is defined as the ability to ensure that information is complete and unaltered and to ensure that it has not been tampered with by any unauthorized person (ISO/IEC, 2013). The Colonial Pipeline attack affected the integrity in the following ways;

1. **Unauthorized Modifications**: The ransomware attacks altered files, configurations and system settings which compromises the systems and data (CISA, 2021).
2. **Potential Data Corruption**: File encryption can sometimes cause data loss due to corruption during the encryption/decryption process or if the system is abruptly powered off during the attack (Check Point, 2021).

1.8.3 Availability

Accessibility means that information and/or resources should be there and should be available to all authorized users whenever needed. The Colonial Pipeline attack had a profound impact on availability.

1. **Operational Disruption**: Since normal operations contributed to the distribution of ransomware to the IT systems, Colonial Pipeline ceased all operations as a result of the incident (CISA, 2021).
2. **Service Interruptions**: The direct impact of the sabotage was that the activities of the pipeline for some days came to a complete standstill.

1.8.4 Systems, Data, or Users Affected

The systems impacted were Colonial Pipeline's IT environment, focusing on the systems that control the administrative and operational data. The incident affected data concerning pipeline activities, finances, and other important company information. Users impacted were company employees who could not work since they couldn't access some important systems, operational staff who were handling the shutdown, and other parties who relied on the fuel supply chain (Greenberg, 2021).

1.9 Vulnerabilities Exploited

Some of the most common vectors used in ransomware attacks are still unspecified for the DarkSide attack on the Colonial Pipeline; however, the incident elucidates the general tactics often used in this type of attack. Knowledge of these threats is necessary for improving the protection of computer networks and preventing similar attacks in the future.

1.9.1 Phishing Attacks

Phishing is still one of the most commonly used and successful ways to get into a network by hackers (ISO/IEC, 2013). It is for this reason that employees must be educated on the identification of phishing attempts to minimize the chances of such incidents (Verizon, 2021). Colonial Pipeline IT systems may have been infiltrated through phishing.

1.9.2 Unpatched Software

Another frequent approach is to target the software vulnerabilities for which no patches have been released yet. Hackers have probably taken advantage of weaknesses in Colonial Pipeline's

older programs that have not been equipped with the latest security fixes. Companies should adhere to a strong patch management policy to make sure that every system and application has the latest security patch hence limiting the areas of vulnerability that cybercriminals can exploit (CISA, 2021).

1.9.3 Weak Network Security

Poor network security settings and improper compartmentalization of the network greatly expose an organization to ransomware attacks. Network segmentation is a technique of dividing the network into smaller sub-networks each having its security measures. In the case of Colonial Pipeline, if there was poor segmentation in the network, then the ransomware could easily move from the administrative IT systems (Check Point, 2021).

1.9.4 Human Error

The human factor is still one of the crucial issues in the sphere of cybersecurity. It could be a simple human error such as misconfiguration of the systems, ignoring the best practices, or getting caught up in a phishing scam. Such factors include having employees undergo regular training on the current cyber threats and how they can prevent them (IBM Security, 2021).

1.9.5 Actions Taken to Control and Prevent Further Damage

In response to the attack, Colonial Pipeline implemented several measures to control and prevent further damage:

- **Shutdown of Pipeline Operations:** Colonial Pipeline decided to stop its pipeline operations to avoid the further spreading of ransomware and IT systems threats.
- **Engagement of Cybersecurity Experts:** The company also engaged cybersecurity companies and federal agencies such as the FBI and CISA to help with containing and cleaning up the breach.
- **Ransom Payment:** The management of Colonial Pipeline Company felt that the only way to go about it was to pay a sum of about $4 4 million to get the decryption key and resume business.

- **System Restoration and Security Enhancements:** An attempt was made to bring back the systems, strengthen the cybersecurity measures, and undertake a detailed security audit to avoid future attacks (CISA, 2021; Greenberg, 2021).

1.10 Lessons Learned

A lot could be learnt from the attack on the Colonial Pipeline system ransomware attack, especially in the management of cybersecurity. Another crucial issue that can be learned from the incident is the need to strengthen organizations' cyber resilience (Brooks et al., 2018). Since critical infrastructure like fuel pipelines are crucial for the nation's security and economic stability then it is imperative to have tight security measures in place (Brewer, 2013). The enhancement of adequate and detailed crisis management plans and the periodic simulations of the same in cases of cyber threats is crucial (Sutton, 2017).

Another important lesson is the importance of cooperation between the public and private sectors in the case of incidents. The Colonial Pipeline attack showed that the communication between private companies and government organizations, including the CISA and the FBI, can improve the response measures.

Cybersecurity should not be overlooked since it is an investment. Some of the ways organizations should invest in to improve their cybersecurity include; investing in better security technologies, and policies, and maintaining up-to-date software and patches. Also, regular training and sensitization of employees should be carried out (Calder and Watkins, 2020).

In addition, the Colonial Pipeline attack demonstrated the need to have a proper incident response plan. Such plans are reviewed and updated often to ensure that they are as relevant as possible when it comes to new and changing threats (Calder and Watkins, 2020).

Last but not least, the incident highlighted the need for preventive measures in cybersecurity. This involves carrying out frequent vulnerability assessments and penetration testing to ascertain any possible vulnerabilities that can be exploited by threat actors. By integrating the concept of proactive security, it becomes possible to protect the organisation's resources and operational continuity

1.11 Conclusion

The Colonial Pipeline attack is a clear example of how vulnerable and risky cyber threats can be to critical infrastructure. This cyber attack on the American infrastructure systems is one of the most dangerous in history and reveals how vulnerable the key services are when they are targeted by professional hackers. The attack's acute consequences, which were the general shortage of fuel and other negative effects on the economy, emphasized the global interdependence of our current systems and the ripple effect of cybercrimes.

Studying the attack brings several important findings on the characteristics of contemporary cyber threats and the appropriate countermeasures. The DarkSide ransomware group's attack revealed how advanced cybercriminals are in their approach, with double extortion tactics that demand both data encryption and leaking. The financial aspects driving the attack, and the operational chaos caused by the shutdown highlighted that companies face two risks: the financial and the services-related ones.

Regarding the attack, Colonial Pipeline's decision to halt the operations and pay the ransom, however unpopular, demonstrated that sometimes, critical services need to be restored using any means possible. The retrieval of part of the ransom by the FBI was an indicator of the efficiency of the police in combating cybercrime (Schou and Hernandez, 2015).

The attack revealed the importance of partnerships between the private and public sectors in strengthening cybersecurity (Brewer, 2013). The public and private sectors can work together to enhance the defences as well as cooperation during the occurrence of a cyber threat. Thus, the experience of this attack should serve as a basis for essential changes in the sphere of cybersecurity and a preventive approach to the protection of national interests in the context of the growing role of digitalization.

2. Part 1B - Cyber Kill Chain

2.1 Possible Cyber Kill Chain for the Colonial Pipeline Attack

The Cyber Kill Chain defines the stages of a cyber attack from the initiation of the attack to the final phase of the attack impact. Below is a possible representation of the Cyber Kill Chain following the events of the Colonial Pipeline Ransomware attack:

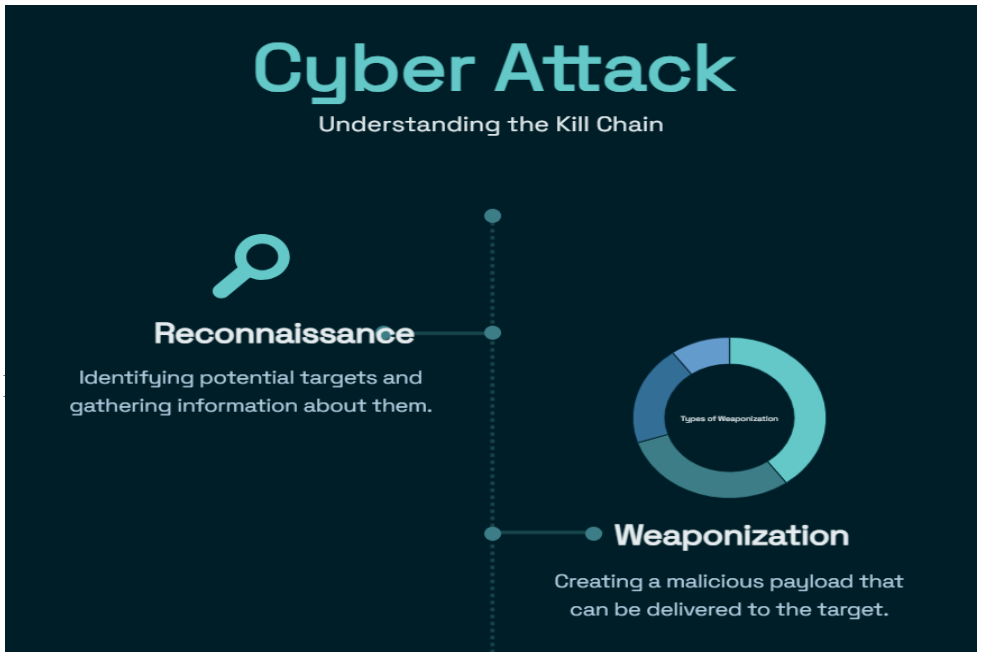
1. **Reconnaissance**
    - **Description:** The attackers conduct a reconnaissance of the Colonial Pipeline's IT and IT environment (Buchanan, 2011).
    - **Methods:** Free internet services, social engineering, and job descriptions to identify system information.
2. **Weaponization**
    - **Description:** The attackers develop or obtain the ransomware itself and the means of its delivery.
    - **Methods:** Creating a new type of ransomware that targets certain weaknesses in the pipelines' IT systems (Chapple, Stewart and Gibson, 2018).
3. **Delivery**
    - **Description:** The ransomware is spread into the target network in some way. This step is characterized by the destruction of the network defence.
    - **Methods:** Thus, for the Colonial Pipeline Company, it is most likely that a series of spear-phishing attacks were used to gain the first entry (CISA 2021).
4. **Exploitation**
    - **Description:** Attacking the target systems with the view of exploiting the available weaknesses with a view of delivering the ransomware..
    - **Methods:** Leveraging on already identified software flaws or using easy-to-guess passwords to get deeper and launch ransomware attacks (Check Point, 2021).
5. **Installation**
    - **Description:** The ransomware is then dropped onto the affected systems and will then go into the stage of persistence followed by encryption.

- **Methods:** It is for this reason that system installation scripts or remote administrative utilities are employed to ensure that the ransomware keeps on running once the system has been restarted (Buchanan, 2011).

6. **Command and Control (C2)**
    - **Description:** The ransomware sends out a communication to the attacker's control and command servers to obtain further directives or for the laundering of the data (Chapple, Stewart and Gibson, 2018).
    - **Methods:** Such links are used to try not to attract attention and transfer information (Greenberg, 2021).
7. **Action on Objectives**
    - **Description:** The last stage is to deliver the payload of the ransomware, this entails encrypting files and presenting a demand for a ransom. This step creates an operational problem (Brooks et al., 2018).
    - **Methods:** Some of them include the encryption of sensitive data and files, coupled with notes that demand a particular sum for the decryption of the files and systems in question (Boulton, 2021).

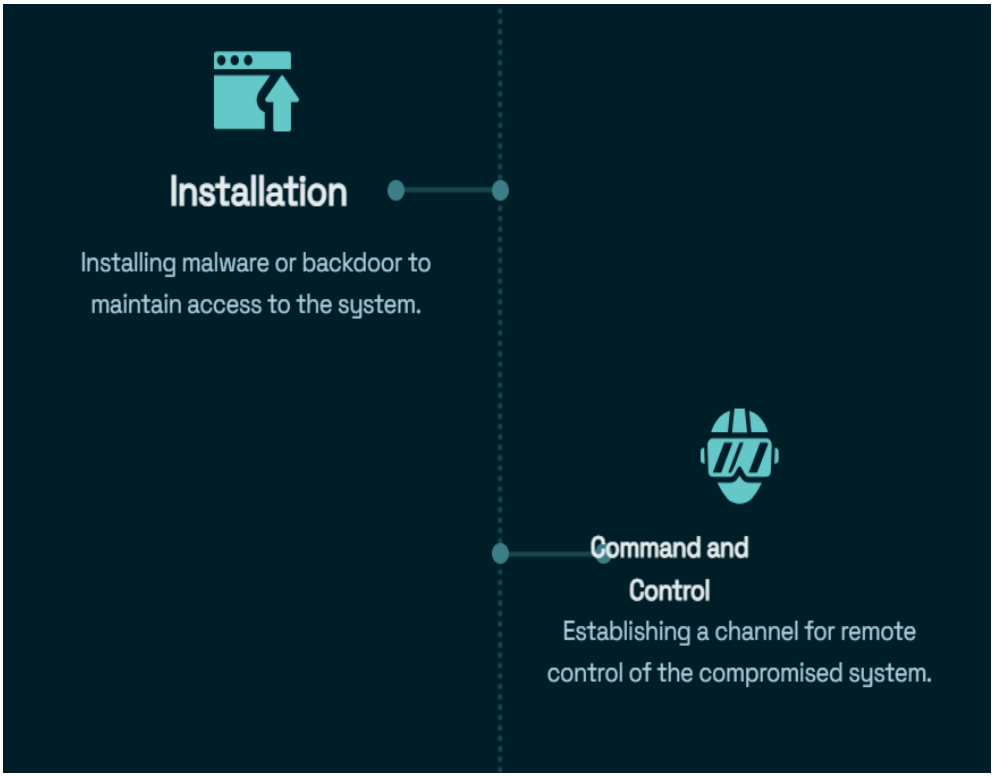
2.2 Diagrammatic Representation of the Proposed Cyber Kill Chain

Reconnaissance and Weaponization

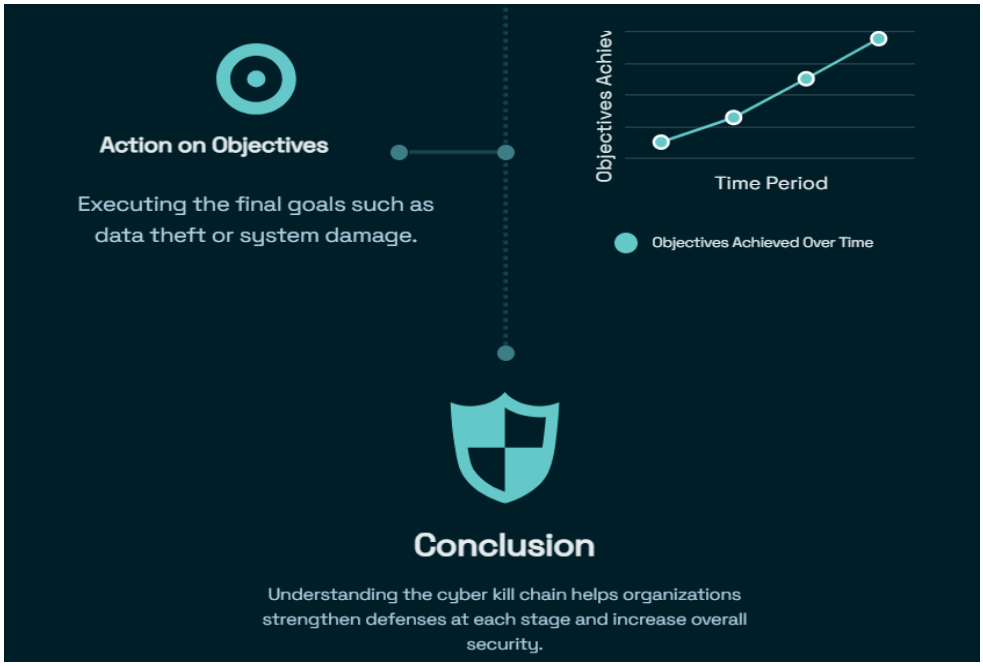


Delivery and Exploitation

Installation and Command & Control



Actions on Objectives And Conclusion



3. Part 2 - Disaster Recovery and Business Continuity

3.1 A. Incident Explanation

The biggest outage in Fastly, a large CDN provider, happened in June 2021 due to a software code push mistake. This attack affected a lot of availability of many popular websites and online services such as news websites and social media platforms. This incident took about one hour and in one hour most of the affected services must have been partially or fully out of service. Fastly was able to identify the cause of the configuration issue and fixed it to get back to normal operations (Fastly, 2021).

3.2 B. Incident Response and Disaster Strategies

1. **Immediate Incident Response**:
    - **Detection and Alerting:** An appropriate program through which the CDN activities, trends and challenges that may be encountered in the CDN should be monitored and the information fed to the IT department.
    - **Root Cause Analysis:** Identify in the shortest time possible the type of crisis that has occurred and the impacts it had.
2. **Disaster Recovery Planning**:
    - **Redundancy:** To make sure that your service is not going to be unavailable due to the failure of one CDN, use several CDNs, or at least have other ways of caching.
    - **Backup Configurations:** It is recommended to configure the scheduled backup of the configuration settings and deployment scripts to prevent issues that can cause massive outages.
3. **Communication**:
    - **Internal Communication:** This a clear guideline that needs to be laid down on how communication is to be made within the company during the occurrence of the incident.
    - **Customer Communication:** Identify the measures to be taken to communicate to the affected users about the developments of the outage, the effects and the possible durations.
4. **Post-Incident Review**:
    - **Lessons Learned:** Conduct a post-incident analysis to determine the cause of the incident and the success of the response, and make changes to the procedures as a result.
    - **Continuous Improvement:** Propose changes to address the findings of the review to strengthen the organization’s ability to manage incidents and prevent such incidents in the future.

3.3 C: Business Continuity Information Security Policy Document

Business Continuity and Disaster Recovery Policy

1. Purpose

This policy document aims to identify ways of maintaining business operations and recovery from a critical incident in case of an instance like a failure of a major CDN. This document shall help minimize the downtime of the organization's services and ensure the availability of critical services.

2. Scope

This policy applies to all departments and employees involved in managing and maintaining the IT infrastructure and CDN services and makes sure that all the relevant parties understand their part in the case of a CDN outage.

3. Incident Response

- **Detection:** Real-time monitoring of the delivery of services to check on any form of deviation. It should be pointed out that the automated alert systems should inform IT teams about possible interruptions (Buchanan, 2011).
- **Response Team:** Determine a group that will be responsible for coming up with a response regarding the outage incident if it occurs. The members of this team should include the IT officials, the communication officials and the senior officials of the company.
- **Root Cause Analysis:** First of all, it is necessary to understand the reason for the disruption in detail. Implement the identified troubleshooting steps to find the cause of the problem and get it fixed as soon as possible (Buchanan, 2011).

4. Disaster Recovery Strategies

- **Redundancy:** It is recommended to conclude the service agreements with several CDN providers to switch to the second one in case the first one does not work properly. Implement a failover system that will allow a move over to the backup CDNs.

- **Backup:** It is advisable to create backups for the CDN configurations, scripts, etc., quite often. With this, ensure that the backups are well secured, and one can easily get them in case there is any need to retrieve them.
- **Testing:** The following should be done to evaluate the efficiency of the given measures for disaster response plans: Schedule the plans to be implemented. Check if the CDN is operable by conducting tests that will cause the CDN to go down to see if the backup and failover are working correctly.

5. Communication

- **Internal Communication:** Develop a plan to be followed when it comes to engaging the right teams at times of disruption. It is recommended to adhere to the established channels and steps so that the transfer of information would be efficient (Buchanan, 2011).
- **Customer Communication:** Develop a customer communication plan that can assist in passing information to the clients during outages. Inform the public regularly on the situation concerning the outage and the estimated time of restoration. Propose to manage the customers' expectations by modifying the implementation of the promises.

6. Post-Incident Review

- **Review:** It is recommended to carry out an analysis of the incident to determine the adequacy of the response as well as the possibilities for its enhancement. It is necessary to document the findings and updates of the policies and procedures.
- **Continuous Improvement:** Make adjustments as suggested in the review and promote the organization's resilience and response measures. It is recommended to perform the business continuity plan regularly and update it to address new threats and risks. (Fastly, 2021)

7. Policy Review and Updates

This policy will be reviewed annually or following any adverse event which has affected the implementation of the policy. Changes will be made from time to time to incorporate more recent

data as well as enhance the already existing information on business continuity and disaster recovery.

8. Responsibilities

- **IT Department:** Also, it is also involved with the setup of monitoring, management of incidents and guarantee of backup and redundant strategies.
- **Management:** Assist in the carrying out of the business continuity planning processes, assist in managing incidents and ensure that the funds allocated for business continuity are well spent for disaster recovery.

4. Part 3 - Security Management Questions

4.1. Benefits of ISO/IEC 27001 Certification

This part focuses on ISO/IEC 27001 which is an International Standard that provides guidance on Information Security Management System which is the process of protecting an organization's information. Achieving ISO/IEC 27001 certification offers several benefits and a few of them are as follows:

4.1.1. Enhanced Security

ISO/IEC 27001 certification assures that an organization has adopted a framework of the necessary measures to protect its information resources. This includes the aspects of risk management, security measures, and incident handling that enhance the organization's security posture against data breaches and cyber threats (ISO, 2022).

4.1.2. Compliance and Legal Requirements

This is based on the ISO/IEC 27001 which is an International Standard that deals with Information Security Management Systems, that is, the management of information security in

an organization. Implementing recommendations about this offers both compliance and security benefits.

4.1.3. Improved Risk Management

ISO/IEC 27001 offers a framework for managing information security risk which enables an organisation to identify its information security risks, and evaluate and treat them. The risk management framework helps in identifying the possible risks and takes measures in advance to avoid them and strengthen security (Jones & Ashenden, 2021).

4.1.4. Increased Trust and Reputation

Gaining cybersecurity certification assures the management and stakeholders of an organization of its preparedness and ability to uphold the best practices of information security. It can enhance the credibility among clients, partners, and other stakeholders creating a possibility to gain more business and competitive advantages (Burt & Williams, 2020).

4.1.5. Continuous Improvement

The standard encourages a culture of regular revision of the security policies and controls to meet the changing environment. This cyclic approach assists organizations in coping with the changing threats and advancements in technologies and hence sustaining sound security mechanisms in the future (ISO, 2022).

4.1.6. Structured Incident Management

ISO/IEC 27001 presents the requirements for developing and implementing incident management processes. This prepares organizations to be ready to address security incidents to reduce the effects that they cause and help in the recovery process (Jones & Ashenden, 2021).

4.2. Type of Audit for the Colonial Pipeline Incident

In the case of the Colonial Pipeline ransomware attack, a **Post-Incident Forensic Audit** would be suitable. This type of audit is conducted to gain insight into the specifics of the attack that has just occurred to establish the extent of the breach, which systems were compromised, and how the breach can be avoided in the future.

4.2.1. Purpose

The main objective of a post-incident forensic audit is to acquire comprehensive information concerning the tactics used in the attack. This entails determining the tactics that the attackers employed, the techniques they used, and the consequences on the organization's systems and information assets (CISA, 2021).

4.2.2. Scope

The audit should cover:

- **Incident Timeline:** Establishment of the event sequences in the attack in an attempt to set out the most likely event sequence that may take place.
- **Vulnerability Assessment:** This means that one has to establish the weaknesses that have been exploited in the security system.
- **System Forensics:** Therefore, to determine the manifestations of the mentioned malicious activities and changes in the data, the systems analysis has to be performed.
- **Access Logs:** Examining the logs that demonstrate the entry points into the network and the passages that the hackers are using.
- **Data Exfiltration:** Find out if the attackers can have obtained information from the organization which was attacked (Check Point, 2021).

4.2.3. Approach

1. **Evidence Collection:** Ensuring that one can seize all the digital evidence that can be influenced by the attack including logs, configurations, and malware samples.

2. **Analysis:** To discover what sort of attack was made and how it was made, the implication of forensic tools and techniques should be used to analyze the information that was collected in the previous steps.
3. **Reporting:** Based on the findings made from the information collected during the event, bringing the activity to a close and preparing a report which may entail among other things a brief description of the event, the effects and the preventive measures that can be taken in the future to increase the security level.
4. **Recommendations:** It is recommended to minimize the effects of the above risks and at the same time improve the management of the occurrence of such incidents (Greenberg, 2021).

4.2.4. Follow-Up

The organization needs to revise its incident handling plan, strengthen its security measures, and educate its employees not to trigger similar incidents in the future.

4.3. Risk Management Process for the Fastly CDN Outage

4.3.1. Risk Identification

- **Incident Identification:** Describe the types of CDN outages mentioning the possible consequences such as service outage, basic loss of availability, and customer experience degradation.
- **Potential Threats:** Identify risks that can be technical for instance system or network failures, and misconfiguration among others that are cyber risks like hacking.

4.3.2. Risk Assessment

- **Likelihood:** Think of how possible it is for a CDN to be taken offline. It is necessary to examine characteristics of the past, present and possible issues in the given area.

- **Impact:** Determine the effects on the business operations, the length of time that the business will be inconvenienced, the revenue that will be affected and the customers' complaints (Fastly, 2021).

4.3.3. Risk Mitigation

- **Redundancy:** One should try to use several CDNs or backup services to prevent the issues with the primary CDN from affecting the service.
- **Configuration Management:** This paper also suggests that it is advisable to conduct the assessment of the configuration parameters frequently and to conduct tests as implied by the best practices of deployment.
- **Monitoring:** CDN should be monitored from time to time for performance and issues that need to be solved.

4.3.4. Risk Response

- **Incident Response Plan:** It is necessary to create and regularly update the incident response plan that will be dedicated to CDN failures. Outline measures on how to prevent, report and deal with such occurrences.
- **Communication:** Ensure that there are proper ways of communicating within the internal teams and the customers to pass on information in case of an outage.

4.3.5. Risk Review and Improvement

- **Post-Incident Analysis:** It is advisable to carry out post-incident action after each power outage to evaluate the efficiency of the response to the incident, to define the issues and to make corrections.
- **Continuous Improvement:** It is suggested to improve the efficiency and reduce the effect of the following outages by modifying the risk management methods which have been derived from the experience.

5. References

Bosworth, S., Kabay, M.E. and Whyne, E., 2014. Computer Security Handbook. 6th ed. NJ: John Wiley and Sons Inc.

Boulton, C., 2021. Colonial Pipeline cyberattack: Here's what you need to know. CIO. Available at: https://www.cio.com/article/3526430/colonial-pipeline-cyberattack-heres-what-you-need-to-know.html [Accessed 21 July 2024].

Brewer, D., 2013. ISO/IEC 27001 Mastering Risk Assessment and the Statement of Applicability. David Brewer.

Brooks, C.J. et al., 2018. Cyber Security Essentials. John Wiley and Sons, Inc.

Buchanan, W.J., 2011. Introduction to Security and Network Forensics. CRC Press.

Burt, R. and Williams, J., 2020. ISO/IEC 27001:2022 - A Comprehensive Guide. London: Kogan Page.

Calder, A. and Watkins, S., 2020. IT Governance: An International Guide to Data Security and ISO27001/ISO27002. 7th ed. London: Kogan Page Limited.

Chapple, M., Stewart, J.M. and Gibson, D., 2018. CISSP Certified Information Systems Security Professional: Official Study Guide. 8th ed. Indianapolis: John Wiley and Sons Inc.

Check Point, 2021. The Colonial Pipeline Attack: A Deep Dive. Available at: https://blog.checkpoint.com/2021/05/10/the-colonial-pipeline-attack-a-deep-dive/ [Accessed 21 July 2024].

CISA, 2020. Remote Access: Security and Implementation. Cybersecurity and Infrastructure Security Agency. Available at: https://www.cisa.gov/publication/remote-access-security [Accessed 21 July 2024].

CISA, 2021. Ransomware Attack on Colonial Pipeline: Alert AA21-131A. Cybersecurity and Infrastructure Security Agency. Available at: https://us-cert.cisa.gov/ncas/alerts/aa21-131a [Accessed 21 July 2024].

Fastly, 2021. Fastly Incident Report: June 2021. Available at: https://www.fastly.com/resources/june-2021-outage [Accessed 21 July 2024].

Greenberg, A., 2021. How the FBI got Colonial Pipeline's ransom back. Wired. Available at: https://www.wired.com/story/how-the-fbi-got-colonial-pipelines-ransom-back/ [Accessed 21 July 2024].

IBM Security, 2021. Cost of a Data Breach Report 2021. Available at: https://www.ibm.com/security/data-breach [Accessed 21 July 2024].

ISO, 2022. ISO/IEC 27001:2022 Information security, cybersecurity, and privacy protection. Available at: https://www.iso.org/standard/82875.html [Accessed 21 July 2024].

ISO/IEC, 2013. International standard ISO/IEC 27001 Information technology – Security techniques – information security management systems – Requirements: Switzerland: ISO/IEC.

Jones, A. and Ashenden, D., 2021. ISO/IEC 27001:2022 Explained. Oxford: Wiley.

NIST, 2021. Guidelines on Securing Legacy Systems. National Institute of Standards and Technology. Available at: https://www.nist.gov/publications/guidelines-securing-legacy-systems [Accessed 21 July 2024].

PwC, 2021. Supply Chain and Cybersecurity. PricewaterhouseCoopers. Available at: https://www.pwc.com/gx/en/services/supply-chain/supply-chain-and-cybersecurity.html [Accessed 21 July 2024].

Schou, C. and Hernandez, S., 2015. Information Assurance Handbook: Effective Computer Security and Risk Management Strategies. 1st ed. McGraw-Hill Education.

Sodhi, M., 2021. The Impact of ISO/IEC 27001 on Compliance and Security. Journal of Information Security, 12(4), pp. 155-169.

Sutton, D., 2017. Cyber Security - A Practitioner's Guide. Swindon: BCS Learning & Development Ltd.

Verizon, 2021. 2021 Data Breach Investigations Report. Available at: https://www.verizon.com/business/resources/reports/dbir/ [Accessed 21 July 2024].