BOSTON UNIVERSITY

Cybersecurity Incident Response Plan

Case Name: Colonial Pipeline Attack

Developed by: Katie Barnes

Date: December 12, 2021

PURPOSE

On May 7, 2021, the Colonial Pipeline Company proactively shut down its pipeline in response to a ransomware attack (DOE, 2021). The cyber-attack targeting Colonial Pipeline has triggered a comprehensive federal response focused on securing critical energy supply chains (The White House, 2021). The Colonial Pipeline Company, our Nation's trusted fuel source and critical infrastructure consisting of 5,500 miles of pipeline that are designed to safely deliver refined products to 7 major airports, 90 military installations, and 270 delivery terminals across the South and East (Felt, 2014). The Colonial Pipeline company delivers more than 105 million gallons of fuel to American businesses, families, and the military every day (Felt, 2014). The Pipeline Company stores information related to consumers, such as names, contact information, birth dates, Social Security, driver's license information; and Military ID numbers and health insurance information (Fung,2021) All of this data information is confidential and unavailable to the public.

On Behalf of the Department of Homeland Security, TSA serves as the co-Sector Risk Management Agency alongside DOT and the United States Coast Guard for Transportation Systems Sector-focused cybersecurity initiatives, programs, assessment tools, strategies, and threat and intelligence information sharing products that support the implementation of Executive Orders on cybersecurity (*United States House of Representatives*, 2021). The Department of Homeland Security has a Cybersecurity plan that is used to detect and respond to unauthorized access or disclosure of private information from systems utilized, housed, maintained, or

serviced by the

Department of Homeland Security. More specifically, this plan defines the roles and responsibilities of various Homeland Security staff with respect to the identification, isolation, and repair of data security breaches to critical infrastructures, outlines the timing, direction, and general content of communications among affected stakeholders, and defines the different documents that will be required during various steps of the incident response. Additionally, TSA is in collaboration with the Department of Defense, and CISA exploring ways in which immediate threats, such as ransomware, can be mitigated through additional cybersecurity measures to ensure that critical pipeline owners and operators are engaging in baseline cyber hygiene and have contingency plans to reduce the risk of significant disruption of operations, if a breach occurs (*United States House of Representatives*, 2021).

The Department of Homeland Security also implements practices designed to proactively reduce the risk of unauthorized access or disclosure, such as training staff with respect to legal compliance requirements, following appropriate physical security and environmental controls for technical infrastructure, and deploying digital security measures such as firewalls, malware detection and several other industry standard systems. In the event of a cyber security incident, the Department of Homeland Security staff have been trained to expeditiously deal with the matter. The Department of Homeland Security staff are trained on a yearly basis to recognize anomalies in the systems they regularly utilize, and to report any such anomalies as soon as possible to the Incident Response Manager so the Incident Response Team can be mobilized. Throughout the year the Incident Response Manager and members of the Incident Response Team are kept up to date on the latest security threats and trained in modern

techniques of incident remediation.

DEFINITIONS

Cyber Security Incident -

A Cyber Security Incident is any event occurring on or conducted through a computer network that actually or imminently threatens the confidentiality, integrity or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon (CISA,2016).

Significant Cyber Incident –

A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people (CISA, 2016).

Cybersecurity-

Our cybersecurity team serves to protect (and, if needed, restore) computer networks, electronic communications, information, and services from damage, unauthorized use, and exploitation. More commonly referred to as information security, these activities ensure the security, reliability, confidentiality, integrity, and availability of critical information, records, and communications systems and services through collaborative initiatives and efforts (CISA,2016).

Forensics and Attribution-

In the context of a cyber incident, forensics refers to several technical disciplines related duplication, extraction, and analysis of data to uncover artifacts relevant to identifying malicious cyber activity. Forensics includes several sub-disciplines, including host-based forensics, network, and packet data forensics (CISA, 2016).

Infrastructure Systems –

Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity. The goal is to stabilize infrastructure assets and entities, repairing damaged assets, regaining control of remote assets, and assessing potential risks to the critical infrastructure sector at large (CISA, 2016).

Interdiction and Disruption –

Delay, divert, interrupt, halt, apprehend, or secure threats related to malicious cyber activity. In the context oof a cyber incident, these threats include people, software, software, hardware, or activities that pose a threat to the Nation’s cyber networks and infrastructure (CISA, 2016).

Logistics and Supply Chain Management-

Facilitate and assist with delivery of essential commodities, equipment, and services in support of responses to systems and networks impacted by malicious cyber activities (CISA, 2016).

Operational Communication-

Ensure the capacity for timely communications in support of security, situational awareness, and operations, available, among and between entities affected by the malicious cyber activity and all responders as far as all levels of government authorized participating private sector partner organizations (CISA, 2016).

CYBER SECURITY INCIDENT RESPONSE TEAM

Our Cyber Security Incident Response Team is a group of experts that assess cyber incidents to protect the securities and vulnerabilities of the United States of America. We serve to protect our Nation's critical infrastructures, assets, data, and protect the wellbeing of our citizens. It is our primary goal to protect our government entities and affiliated partnerships as well as the people of our nation. Our Cyber Security Incident Response Teamwork are working with top tier authorities and utilize top of the line software to delineate any threats to our country's critical infrastructures.

INCIDENT RESPONSE MANAGER

The incident response manager oversees and prioritizes actions during the detection, analysis, and containment of an incident. The incident response manager handles high severity incidents foreseeing the entire department.

TECHNICAL CONTACTS

The contact information for DHS Headquarters is as follows:

- Operator number: 202-282-8000.
- Comment Line: 202-282-8495.
- TTY: Use the Federal Relay Service for either number above.
- DHS Mailing Address.

LEGAL COUNSEL

The Office of the General Counsel:

- Provides complete, and accurate, and timely legal advice on possible courses of action for the Department.
- Ensuring that Homeland Security policies are implemented lawfully, quickly, and efficiently.
- Protecting the rights and liberties of any Americans who come in contact with the Department.
- Facilitating quick responses to congressional requests for information; and
- Representing the Department in venues across the country, including in U.S. immigration courts (DHS,2021).

DHS Rulemaking

"DHS mission is to ensure a homeland that is safe, secure, and resilient against terrorism and other potential threats.

In many cases, DHS carries out its mission through the promulgation of regulatory actions. The DHS regulatory agenda includes regulations issued by DHS components, including the following seven operational components with regulatory responsibilities:

- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard (USCG)
- U.S. Customs and Border Protection (CBP)
- Federal Emergency Management Agency (FEMA)

- U.S. Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- Cybersecurity and Infrastructure Security Agency (CISA)

DHS is committed to ensuring that all regulatory initiatives are aligned with its guiding principles to protect civil rights and civil liberties, integrate our actions, build coalitions and partnerships, develop human resources, innovate, and be accountable to the American public (DHS, 2021)."

LEGAL AUTHORITIES

"The following legal authorities provide some of the major requirements for the federal rulemaking process:

- The Administrative Procedure Act (APA), 5 U.S.C §551 *et seq*. governs the process by which federal agencies develop and issue regulations.
- The Regulatory Flexibility Act (RFA), 5 U.S.C. §601 et seq. requires federal agencies, when developing proposed and final regulations, to consider the impact of regulations on small entities.
- Executive Order 13272, "Proper Consideration of Small Entities in Agency Rulemaking" directs agencies to establish procedures and policies to promote compliance with the Regulatory Flexibility Act.
  • DHS has "Procedures for Compliance with the Regulatory Flexibility Act and Executive Order 13272" (November 3, 2004), which provides DHS with guidance for meeting the requirements of the RFA and Executive Order 13272."
- Executive Order 12866 "Regulatory Planning and Review" and Executive Order 13563 "Improving Regulation and Regulatory Review" *(PDF - 3 pages. 144 KB)* direct federal agencies to follow certain principles in rulemaking, such as the consideration of alternatives and careful analysis of benefits and

costs and describes the Office of Information and Regulatory Affairs' role in the federal rulemaking process.

- Executive Order 13771 "Reducing Regulation and Controlling Regulatory Costs" requires federal departments and agencies to: (1) eliminate two regulatory actions for each new regulatory action; and (2) not exceed a regulatory cost allowance (DHS,2021)."

COMMUNICATIONS SPECIALIST

Homeland Security Communication Specialist general role and responsibility is to handle public relations, information output, press releases and media requests, social media and/or advertising efforts.

ADDITIONAL MEMBERS

In addition to those individuals listed above, additional experts may be included on the DHS staff, depending upon the nature and scope of the incident. For instance, the level of the cyber security measures and dangers to the public. Our expert teams will evaluate every situation big or small in a professional and discrete manor.

INCIDENT MANAGEMENT **PRINCIPLES**

CONFIDENTIALITY

1. Investigation

During a Cyber Security Incident investigation, DHS or members of the DHS will be gathering information from multiple computer systems and/or conducting interviews with key personnel based on the scope of the incident in question. All information and data collected are kept confidential and handled by professionals. Throughout the Cyber Security Incident investigation, no confidential information shall be shared unless it pertains to the incident. DHA follows strict privacy guidelines and assure the privacy to all members of staff and other entities involved. At the conclusion of the investigative process, the DHS will brief District Administration on the relevant details of the incident and the investigation (see Briefing of Administration in the Response Phase).

2. Affected Stakeholders

TSA's focus on pipeline security began in 2001 and through our expanding efforts, we have focused on enhancing the security preparedness of the Nation's hazardous liquid and natural gas (Testimony, June 15, 2001). If private data is breached TSA has established a productive public-private partnership and readiness plan with government partners and the pipeline industry. TSA collaboratively develops security guidelines and training materials in Security Directives (SD) and training materials through cybersecurity assessments shared with pipeline industry partners to increase security awareness and preparedness (*United States House of Representatives*, 2021).

In the event any incident involves information of a non-stakeholders, such as a neighboring district or vendor partner, TSA Homeland Security will take appropriate steps to notify those entities as efficiently as possible.

In the event the incident is limited to affiliated systems not containing sensitive or confidential information, it will be the discretion of the Homeland Security TSA administration and the Department of Defense whether to share information related to the incident with outside stakeholders.

3. Report Management

All reports generated during an investigation along with any evidence gathered will be stored and managed by the Department of Homeland Security and all authorized agencies. Any physical records are confidential and accessible only by authorized personnel. Any digital records will be stored, sealed, and protected by the Department of Homeland Security. All data will be backed up and stored in accordance with policies and laws of the United States Government agencies. In the event past records of incidents need to be reviewed, a written request must be made to the Department of Homeland Security that includes the requestor, the information requested and the reason for the request. The Department of Homeland Security will review the request and has the discretion to approve or deny any request.

COMMUNICATION GUIDELINES

- Communication with government agencies or other authorized entities such as the Colonial Pipeline Company, will be disseminated via the Department of Homeland Security.

- All Cybersecurity incidents follow a strict chain of command and follow strict protocols.

- Initial communication to affected stakeholders should occur as expeditiously as possible upon the identification of the incident. In some cases, this may include an initial communication (letter, email, phone call) that simply states that our National Cyber Security agency (The Department of Homeland Security) is aware of the issue and is addressing it, with the promise of a follow up in accordance with agency procedures.

    - Should the unauthorized release of personnel data occur, DHS shall notify all employees or entities affected by the release in the most expedient way possible.

    - Should the unauthorized release of protected staff data occur, the Department of Homeland Security shall notify the staff members and affiliated groups affected by the release in the most expedient way possible.

- Should the release of Social Security Number, Driver's License or Non-Driver ID Number, Account Number, or Credit/Debit Card number combined with other sensitive information occur all sensitive information will be handled with care (discreetly) and quickly according to federal laws.

- Updated communications will come from the chief of staff or the Incident Response Manager. As staff receive requests from all departments for information, they should pass those requests along to the Incident Response Manager of the DHS.

- District staff (Chief of staff) should be clearly informed by the Management Team what information is public and what is internal confidential. However, department leadership should be aware that any material or information communicated to staff can and likely will be shared with the public, including the news media.

- Communication with news media will be initiated by our own Communication Specialist and/or designee. Incoming news media calls and requests for information will be directed through the Department of Homeland Security Incident Response Team Communication Specialist. A communication response plan (talking points, interview refusal statement, etc.) will be formulated as needed, with information coming from the chief of staff or designee.

CYBER SECURITY INCIDENT PHASES

IDENTIFY

Overview

All DHS staff have a responsibility to remain vigilant and protect the data stored within the systems we support. Any event that threatens the confidentiality, integrity, or availability of the information resources we support or utilize internally should immediately be reported to the team leader or supervisor of the cyber security department.
Supervisors should immediately bring the incident to the attention of the Chief of Homeland Security staff in the cyber security department. Staff and other affiliated entities are encouraged to notify DHS of possible breaches or other government referenced in this cyber security incident response plan (see Appendix G).

Incident Types

Types of cyber incidents that may threaten the organization are:

- Unauthorized attempts to gain access to a computer, system, or the data within
- Service disruption, including Denial of Service (DoS) attack
- Unauthorized access to critical infrastructure such as servers, routers, firewalls, etc.
- Virus or worm infection, spyware, or other types of malware
- Non-compliance with security or privacy protocols
- Data theft, corruption, or unauthorized distribution

Incident Symptoms

Signs a computer may have been compromised include:

- Abnormal response time or non-responsiveness
- Unexplained lockouts, content, or activity
- Locally hosted websites won’t open or display inappropriate content or unauthorized changes
- Unexpected programs running
- Lack of disk space or memory
- Increased frequency of system crashes

- Settings changes
- Data appears missing or changed
- Unusual behavior or activity by the Department of Homeland Security staff, relatives of staff, partners or other actors should be reported to a supervisor immediately.

ASSESS

Overview

Once anomalous activity has been reported, it is incumbent upon the DHS to determine the level of intervention required. Other members of the DHS may be required to provide input during this phase to help determine if an actual security threat exists. If it is determined there is an active security threat or evidence of an earlier intrusion, the DHS will alert the entire department immediately so that the situation may be dealt with as expeditiously as possible.

Considerations

- What are the symptoms?
- What may be the cause?
- What systems have been / are being / will be impacted?
- How widespread is it?
- Which stakeholders are affected?

Documentation

Regardless of whether it is determined there is a security threat, the Department of Homeland Security will accurately document the scenario in a Cyber Security Incident Log. All Cyber Security Incident Logs will be stored in a single location so incident information may be reviewed in the future. This report should contain information such as:

- Who reported the incident
- Characteristics of the activity
- Date and time the potential incident was detected

- Nature of the incident (Unauthorized access, DDoS, Malicious Code, No Incident Occurred, etc.)
- Potential scope of impact
- Whether the DHS is required to perform incident remediation?

RESPOND

Briefing of Administration

When the Department of Homeland Security determines that a significant cyber security breach has occurred our mission is to mitigate the situation as fast as possible. The head of the department (Chief of Homeland Security Cyber Security Division) should be notified immediately. Our primary goal is to save lives, protect property and the environment, as well as meeting the basic needs of a community during a disaster (DHS, cyber incidents). As additional information is uncovered throughout the investigation, Administration should be briefed by the department so appropriate decisions, such as allocating additional staff, hiring outside consultants, and involving law enforcement can be made. Additionally, based on the incident, it will be incumbent on Administration to determine the appropriate stakeholders to notify of the incident and the appropriate medium to do so. Administration should take into consideration the nature of the information or systems involved, the scope of the parties affected, timeliness, potential law enforcement interests, applicable laws and the communication requirements of all parties involved. Sample communications documents may be found in Appendices C - F.

Initial Response

This first steps in any cyber security incident response should be to determine the origin of the incident and isolate the issue. The system and data backup are crucial; however, it may be a short-term strategy considering extensive cleansing, recovery, and investigation time (Choi, Module 6). Planning and organizing are crucial and require both public and private sectors to respond rapidly to the impact of the attack (Choi, Module 6). Constructing a robust incident response plan is vital to proactively prevent a catastrophic cyber-attack (Choi, Module 6). This may involve measures up to and including immediately disconnecting particular workstations, servers, or network devices from the network to prevent additional loss. While this is occurring, it is necessary to examine firewall and system logs, as well as possibly perform vulnerability scans, to ensure the incident has not spread to other areas in order to define the entire scope of the incident.

Throughout this process, it will be critical to preserve all possible evidence and document all measures taken in detail. Thorough review and reporting on the incident will be required once the threat has been removed, the vulnerabilities have been removed and the systems have been restored.

- Phase 1-Planning for Pre-attack
- Phase 2- response and Recovery for Post-attack
- Phase 3-Stand down for post-attack

Cyber Security incidents include:

- Cyber-attacks
- DOS attacks
- Execution of malicious code
- Digital; events such as floods, and tornadoes
- Terrorism

Category	Definition and Explanation
Information Attacks	Cyber terrorist attacks focused on altering or destroying the content of electronic files, computer systems, or the various materials therein.
Infrastructure Attacks	Cyber terrorist attacks designed to disrupt or destroy the actual hardware, operating platform, or programing in a computerized environment.
Technological Facilitation	Use of cyber communications to send plans for terrorist attacks, incite attacks, or otherwise facilitate traditional terrorism or cyberterrorism.
Fundraising and Promotion	Use of the Internet to raise funds for a violent political cause, to advance an organization supportive of violence political action, or to promote an alternative ideology that is violent in orientation

Figure 1: Types of Cyber Terrorism (Choi, Module 2)

Remediation and Recovery

Once the cause has been determined and appropriately isolated, the DHS cyber security department will need to remove the vulnerabilities leading to the incident. This may involve some or all of the following:

- Install patches and updates on systems, routers, and firewalls
- Infections cleaned and removed
- Re-image or re-install operating systems of infected machines
- Change appropriate passwords
- Conduct a vulnerability scan of any compromised machines before reconnecting them to the network
- Restore system backups where possible
- Document all recovery procedures performed and submit them to the DHS
- Closely monitor the systems once reconnected to the network

REPORT

Overview

Once the threat has been mitigated and normal operation is restored, the Department of Homeland Security will compile all available information to produce an accurate and in-depth summary of the incident in an Incident Summary Report (ISR). A copy of the ISR is located in Appendix A. Throughout the incident, DHS will have kept Incident Logs that contain detailed records wherever possible, and these shall serve as the basis of the report. Interviews will also be conducted with appropriate members and affiliated parties of DHS to obtain any additional information that may be available to augment the logs and records kept throughout the process. It is imperative for all participating agencies Additionally, as required by Federal Law of all departments will be required to maintain a record of all complaints of breaches or unauthorized releases of data in accordance with applicable data retention policies using the log in Appendix H.

Report Contents

The Incident Summary Report (ISR) will include all pertinent information to the incident, but at minimum:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Timeframe

DHS should be prepared as expeditiously as possible following the incident so future preventative measures may be taken as quickly as possible. Information to prepare the DHS and interviews with the DHS should be conducted immediately to ensure the greatest possible accuracy of information.

REVIEW

Post-Incident Review Meeting

Upon concluding the cyber incident investigation, the DHS and possibly select members from the DHS will meet with management to discuss the event in detail, review response procedures and construct a Strategic Prevention Plan (SPP) to prevent a reoccurrence of that or similar incidents. The compiled Incident Report constructed by the Department of Homeland Security (DHS) will serve as a guide for this meeting. The inclusion ensures that information security is included in high-level strategic planning and cyber security executives are considering risk assessment along with other strategic planning objectives, including investments and business identifying an information Security structure, and building policies and procedures that protect an organization's most important assets (Dhillon, 2015).

In the meeting, a full debrief of the incident will be presented and findings discussed. DHS will share the full scope of the breach (as comprehensively as possible), causes of the breach, how it was discovered, potential vulnerabilities that still exist, communication gaps, technical and procedural recommendations, and the overall effectiveness of the response plan.

Our cyber security team will review the information presented and will determine any weakness in the process and determine all the appropriate actions moving forward to modify the plan, address any vulnerabilities and what communication is required to various stakeholders.

Strategic Prevention Plan

Even with a perfectly functioning IT governance, it is important to check in with all units to ensure they are following policies and procedures for appropriate computer usage policies governance structure, an effective plan and complying with rules and regulations of the United States government (Dhillon, 2015). The new and improved plan will focus on the following areas:

- New hardware or software required
- Patch or upgrade plans

- Training plans (Technical, end users, etc.)
- Policy or procedural change recommendations
- Recommendations for changes to the Incident Response Plan
- Regional communications recommendations

Additionally, the SPP must be kept strictly confidential for security purposes. Any communication required to clients or to the public must be drafted separately and include only information required to prevent future incidents.

As defenders of our great Nation, we must move ahead of the threat of cyberattacks, it must go beyond traditional security systems, and shift focus to mor preventative solutions (Dhillon, 2015).

- Threat Detection
- Network Traffic Inspection
- Network Segmentation
- Penetration Testing
- Auditing and Monitoring
- Paying attention to personal devices and business devices

APPENDIX A:

INCIDENT SUMMARY REPORT

INCIDENT SUMMARY

Type of Incident	Ransomware attack on the Colonial Pipeline Company.
Date Incident Originated	May 07, 2021
Date Incident Was Detected	May 07, 2021
By Whom Was Incident Detected	Chief of staff (acting) Jennifer Higgins
How Was Incident Detected	Complaint initiated by Colonial Pipeline Company. A threat for ransom in exchange for company data was made by a hacker group called "The Dark Side".
Scope of Incident (Districts / Systems Affected)	The pipeline suffered a ransomware attack that forced the U.S. energy company to shut down its entire fuel distribution pipeline- and therefore threatened gasoline and jet fuel distribution across the U.S. east coast (Panettieri, 2021).
Date Incident Corrected	May 12, 2021
Corrective Action Types (Training, Technical, etc.)	Cybersecurity firm FIREEYE assisted the cyberattack investigation and recovery effort along with multiple agencies (Homeland Security, FBI, CISA, and the Department of Defense.

Initial Complaint

"On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. We have since determined that this incident involves ransomware. In response, we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems. Upon learning of the issue, a leading, third-party cybersecurity firm was engaged, and they have launched an investigation into the nature and scope of this incident, which is ongoing. We have contacted law enforcement and other federal agencies.

Colonial Pipeline is taking steps to understand and resolve this issue. Currently, our primary focus is the safe and efficient restoration of our service and our efforts to return to normal operation. This process is already underway, and we are working diligently to address this matter and to minimize disruption to our customers and those who rely on Colonial Pipeline (Colonial Pipeline, 2021)."

Summary of Incident Type and Scope

On Thursday, May 6, 2021, hackers launched an attack on the Colonial Pipeline Fuel Company Stealing 100 gigabytes of data before locking computers with ransomware and demanding payment in exchange for company data (Panettieri, 2021).

Summary of Corrective Actions

On Saturday, May 8th, 2021, U.S. Government Assists Attack response:
Colonial Pipeline, the White House, The FBI, CISA, NSA and several other U.S. government agencies servers were shut off by the hackers. The Colonial Pipeline data from the United States to alleged hacker locations in Russia (Bloomberg, 2021).

Summary of Mitigation Processes and Internal Communication

Communications Log (Attach drafts for written communications, synopsis for verbal communication)

Communication Date	Communication Type	Recipient(s)	Purpose
May 7, 2021	Official statement of complaint received by the Colonial Pipeline Company.	Chief of Staff- Jennifer Higgins	Initiate Cyber Security Investigations with release to all government agencies for critical infrastructure high level threat.
May 8, 2021	Complaints from the White House, FBI, CISA, and NSA affected by ransomware attack.	Secretary Alejandro Mayorkas	Expedite complaint to all Cyber Security staff.
May 9, 2021	Confirmation the Cybersecurity and Infrastructure Security Agency (CISA) and the Transportation Security Administration are involved in investigation.	Executive Secretary Kimberly O’ Connor	Initiating involved in both public and private sectors

APPENDIX B:

PROCESS IMPROVEMENT PLAN

PROCESS IMPROVEMENT PLAN

Areas of Success Summary

- Properly trained staff
- Ensuring all aspects of the incident response plan (training, execution, hardware, and software resources, etc.) are approved and funded in advance (Ellis, 2021).
- Well documented Incident Response Planning in effect
- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Areas in Need of Improvement Summary

- Preparation
- Organization

Recommended Improvements to Avoid Future Incidents

It is recommended that the chief of security implements new and innovative education and training to all employees. To stay ahead of trends our security need to have top tier education.

Recommended Improvements to the Cyber Security Incident Response Plan

Successful Strategic Planning requires that all members of DHS prepare for cyber incidents because this is the most crucial phase to protect critical infrastructures. Members of DHS are properly trained, organized, and

authorized on all security levels. With every incident big or small is a learning experience therefore to stay on top of new trends and evolving threats all members will closely monitor every incident and fully prepared in every aspect before events occur. This will help our cyber security team response to an incident more effectively in an accelerated expert level.

Improvement	Timeframe	Cost
Prevention Plan	May 2021- December 2021	14,000.00
Organization	December 2021	10,000.00
Education Training	December 31st Deadline 2021	60,000.00
Software/Hardware Tools	Every 6 months	50,000.00 -70,000.00
Recovery Costs	Per Incident	0-100,000.00+

APPENDIX C:

INCIDENT LOG

INCIDENT LOG

Incident Title

Ransomware attack on Colonial Pipeline Company

Incident Opened Date

May 06, 2021

Incident Description

Cyber Attack on Fuel Critical Infrastructure High Level Severity Threat

Action / Event	Date / Time	Performed / Reported by	Details
Initial Complaint by Colonial Pipeline Company	May 06, 2021	Chief of Staff Jennifer Higgins	Loss of access to critical data and sensitive information. Ransom requested for 4 million dollars.
Expediting Infrastructure threat to inform all Cyber Security personnel.	May 08, 2021	Secretary Alejandro Mayorkas	Informing all agents of Critical Infrastructure threat and severity
Initiating involved in both public and private sectors	May 09, 2021	Executive Secretary Kimberly ‘O Connor	Confirmation the Cybersecurity and Infrastructure Security Agency (CISA) and the Transportation Security Administration are involved in investigation.
Communications Operator	May 09, 2021	Jonathan E. Meyer	Securing Confidential Operations
Military Advisor	May 09, 2021	Michael Day	Meeting with all Agencies
Cyber Security Specialist Team Response Manager	May 10, 2021	Rachell Belle	Meeting with CISA
Case Resolved	May 12, 2021	Chief of Staff Jennifer Higgins	Case Resolved data back up and running with fuel pipeline. All entities contacted.
Post Attack Meeting	May 13, 2021		Discuss Losses in revenue and preventative plans.

References

Choi, K. (2021). Module 2: *Technology Use by Extremists & Digital Footprinting*. Boston University

Choi, K. (2021). Module 6: *Countering Cyberterrorism*. Boston University

Cybersecurity & Infrastructure Security Agency (2021). *The National Cyber Incident Response Plan (NCIRP).* [PDF FILE]. Retrieved from: https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

Felt, T. C. (2014). *Quadrennial Energy Review Stakeholder Meeting Transmission, Storage and Distribution Issues Relating to Petroleum and Refined Products*. Energy.Gov. Retrieved December 14, 2021, from URL https://www.energy.gov/sites/prod/files/2014/06/f16/tfelt_statement_qer_nola.pdf

Dhillon, G (2015). The Changing Faces of Cybersecurity Governance. *What to Do Before and After a Cybersecurity Breach* [PDF File]. Retrieved from: https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf

Ellis, D. (2021). *6 Phases in the Incident Response Plan*. Securitymetrics. Retrieved December 18, 2021, From URL: https://www.securitymetrics.com/blog/6-phases-incident-response-plan

Spencer, T. (2019). *How to Recover from a Cyber Attack*. Nist.gov. Retrieved December 18, 2021, From URL: https://www.nist.gov/blogs/manufacturing-innovation-blog/how-recover-cyber-attack

Turton, W. Riley, M. Jacobs, J. (2021). *Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom*. Bloomberg. Retrieved December 16, 2021, from URL https://www.bloomberg.com/cybersecurity

United States Department of Energy (2021). Office of Cybersecurity, Energy Security, and Emergency Response. *Colonial Pipeline Cyber Incident*. Retrieved from https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

United States House of Representatives *Cyber Threats in Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack*, One Hundred Seventeenth Congress First Session Serial No. 117-18. Page 16 (June 15, 2021) Retrieved from: Permalink: https://congressional-proquest-com.ezproxy.bu.edu/congressional/docview/t29.d30.hrg-2021-hsc-217561?accountid=9676