A logo of a person in a hat and a crosshair

Description automatically generatedA person wearing a headset

Description automatically generated

**IR TABLETOP EXERCISE**

AFTER ACTION REPORT

Colonial Pipeline

Included departments include: Information Technology (IT)/Cybersecurity Team; Executive Leadership; and the Legal Department

10/07/2024

# Executive Summary

## Introduction

## Exercise Objectives

The primary objective of the exercise was to test the incident response plan for a ransomware attack. This included evaluating the team's ability to identify, classify, isolate, eradicate, and recover from the incident.

## Participants

The following participants attended this exercise:

The participants are the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), and the IT Security Manager.

## Exercise Summary

This tabletop exercise was conducted to test Colonial Pipeline's incident response capabilities in the event of a ransomware attack. The scenario was based on a sophisticated ransomware attack similar to the one experienced by Colonial Pipeline in May 2021, involving the hacker group DarkSide. The attackers gained access through a compromised VPN password and encrypted critical information, leading to operational disruptions. The exercise aimed to evaluate the team's response actions, including identification, containment, eradication, and recovery. Overall, the team demonstrated effective incident response capabilities, successfully isolating affected systems and restoring operations. However, there were areas for improvement, particularly in communication and coordination with external partners.

## Injects Used

The SCADA system controlling pipeline flow shows unexpected changes in pressure readings.  
An employee in the control room reports their screen is locked with a ransomware message.  
The billing system becomes inaccessible, potentially compromising customer data.  
Unusual remote access attempts are detected on the VPN used for pipeline monitoring.

# Exercise Results

## Exercise Score

Score: 85 out of 100

## Analysis Summary

The team effectively activated the incident response plan, notified key personnel, and isolated compromised systems. The SCADA system was brought back online with minimal disruption, and the team engaged external consultants for expert assistance. Communication with stakeholders and regulatory authorities was initiated, and insurance claims were submitted. However, there were delays in determining the initial compromise point and in coordinating with external partners for a comprehensive review. The exercise highlighted the need for improved communication strategies and regular tabletop exercises to enhance readiness.

## Positive/Successful Actions

Prompt activation of the incident response plan.  
Effective isolation of compromised systems.  
Successful restoration of SCADA and control room operations.  
Engagement with external consultants for expert assistance.  
Submission of insurance claims and SEC 8-K disclosure.

## Areas for Improvement

Delays in determining the initial compromise point.  
Need for improved coordination with external partners and regulatory authorities.  
Enhancement of communication strategies with stakeholders.  
Regular tabletop exercises to test and improve incident response capabilities.

## Incident Cost Breakdown

Internal team efforts and resource allocation: $300,000  
External consulting fees (Mandiant): $400,000  
System restoration and security enhancements: $200,000  
Customer compensation and communication efforts: $300,000  
Total Cost: $1,200,000

## Score Deductions

Delays in determining the initial compromise point: -5 points  
Need for improved coordination with external partners: -5 points  
Enhancement of communication strategies: -5 points

## Mitre ATT&CK TTPs Used by the Threat

The scenario was based on the DarkSide ransomware attack, which involved the following techniques:  
  
Initial Access: Compromised VPN credentials (T1078)  
Execution: Ransomware execution on IT systems (T1486)  
Persistence: Use of compromised accounts (T1078)  
Lateral Movement: Unauthorized access to network resources (T1021)  
Impact: Data encryption and operational disruption (T1486)

# IR Plan Review

## IR Team Performance

An IR plan was not provided for this exercise.

## IR Plan Gap Assessment

An IR plan was not provided for this exercise.  
Please let me know if you have any further questions or need additional clarification on the exercise results.