



Colonial Pipeline Incident

CASE STUDY ON TABLETOP EXERCISE VS. REALITY

ROBERT C. RHODES

Colonial Pipeline Ransomware Incident

Case Study on Tabletop Exercise vs. Reality

Contents

- Executive Summary.....2
- Background.....2
- Tabletop Exercise Scenario2
- Exercise Response and Outcomes.....3
- Key Actions Taken3
- Positive Outcomes3
- Areas for Improvement.....3
- Comparison with the Actual May 2021 Incident.....4
- Similarities4
- Key Differences.....4
- Lessons Learned and Recommendations4
- Real Life at Colonial Pipeline.....4
- Conclusion5
- Appendix A – AutoTableTop™ Transcript.....6

Executive Summary

This case study examines a cybersecurity tabletop exercise conducted for Colonial Pipeline, simulating a ransomware attack similar to the one experienced in May 2021. The exercise aimed to test the company's incident response capabilities and identify areas for improvement. By comparing the exercise outcomes with the actual incident, we can gain valuable insights into the effectiveness of preparedness measures and the challenges of real-world cyber incidents.

Background

Colonial Pipeline Company operates the largest refined products pipeline system in the United States, spanning over 5,500 miles and supplying about 45% of the East Coast's fuel. In May 2021, the company fell victim to a significant ransomware attack that disrupted operations and caused widespread fuel shortages.

Tabletop Exercise Scenario

The exercise simulated a ransomware attack mirroring the May 2021 incident:

- ✓ Attackers gained access through a compromised VPN password
- ✓ The SCADA system showed unexpected pressure changes
- ✓ Control room screens were locked with ransomware messages
- ✓ The billing system became inaccessible

Exercise Response and Outcomes

Key Actions Taken

- 1) Activated the Incident Response Plan
- 2) Notified key personnel and authorities
- 3) Isolated compromised systems
- 4) Engaged external consultants (Mandiant)
- 5) Restored SCADA and control room operations
- 6) Submitted insurance claims and SEC 8-K disclosures

Positive Outcomes

- ✓ Swift activation of the response plan
- ✓ Effective system isolation and restoration
- ✓ Engagement of external expertise

Areas for Improvement

- ✓ Delays in identifying the initial compromise point
- ✓ Need for better coordination with external partners
- ✓ Enhancement of communication strategies

Comparison with the Actual May 2021 Incident

Similarities

- ✓ Attack vector: Compromised VPN account
- ✓ Systems affected: IT systems, including billing
- ✓ Operational impact: Disruption of pipeline operations

Key Differences

Aspect	Tabletop Exercises	Actual Incident (May 2021)
Response Time	Immediate activation of IR plan	Took several days to fully assess and respond
System Shutdown	Partial, controlled shutdown	Complete pipeline shutdown for 5 days
Ransom Payment	Not addressed in exercise	\$4.4 million paid to attackers
External Assistance	Proactive engagement of Mandiant	Engaged after the incident was detected
Regulatory Involvement	Simulated notifications to DHS, FBI, CISA	Extensive involvement of multiple agencies
Public Impact	Limited simulation of public response	Widespread fuel shortages and panic buying

Table 1 - Key Differences between AutoTableTop™ transcript and real life

Lessons Learned and Recommendations

- 1) Implement multi-factor authentication for all access points, especially VPNs
- 2) Conduct regular security audits and penetration testing
- 3) Enhance employee security awareness training
- 4) Update and regularly test the Incident Response Plan
- 5) Establish clear communication protocols with stakeholders and authorities
- 6) Implement advanced network monitoring and logging systems
- 7) Develop a comprehensive strategy for engaging with external partners during incidents

Real Life at Colonial Pipeline

Based on the [public search results](#) provided, Colonial Pipeline took the following steps in response to the ransomware attack:

- 1) **Shut down pipeline operations:** Colonial Pipeline proactively shut down its entire pipeline system on May 7, 2021, to contain the threat and prevent further spread of the ransomware[1][2].

- 2) **Notified authorities:** The company notified law enforcement and federal agencies, including the FBI, Cybersecurity and Infrastructure Security Agency, U.S. Department of Energy, and Department of Homeland Security[1].
- 3) **Engaged cybersecurity experts:** Colonial Pipeline brought in security investigation firm Mandiant to investigate the attack and respond to the incident[1][3].
- 4) **Paid the ransom:** The company paid a ransom of 75 bitcoin (approximately \$4.4 million at the time) to the DarkSide hackers on May 7, 2021, to obtain a decryption tool[1][3][4].
- 5) **Worked on system restoration:** After receiving the decryption tool, the company worked to restore its systems, though the tool was reportedly slow and required significant time to bring systems back online[4].
- 6) **Restarted pipeline operations:** Colonial Pipeline began restarting pipeline operations on May 12, 2021, with normal operations resuming on May 15, 2021[1][3].
- 7) **Addressed data theft:** The company dealt with the theft of approximately 100 gigabytes of data that occurred during the attack[3][4].
- 8) **Cooperated with recovery efforts:** Colonial Pipeline cooperated with federal authorities, which led to the recovery of 63.7 bitcoin (worth approximately \$2.3 million) by the Department of Justice on June 7, 2021[1][4].

These actions demonstrate that Colonial Pipeline took a multi-faceted approach to address the ransomware attack, focusing on containment, investigation, system recovery, and cooperation with authorities.

Citations:

[1] <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>

[2] <https://www.energy.gov/ceser/colonial-pipeline-cyber-incident>

[3] <https://insurica.com/blog/colonial-pipeline-ransomware-attack/>

[4] https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

[5] <https://www.msspalert.com/news/colonial-pipeline-investigation>

[6] <https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/>

Conclusion

The tabletop exercise demonstrated Colonial Pipeline's improved preparedness since the May 2021 incident. However, the exercise also highlighted the complexity of responding to sophisticated cyber-attacks and the importance of continuous improvement in cybersecurity practices. By addressing the identified areas for improvement and implementing the recommendations, Colonial Pipeline can further enhance its resilience against future cyber threats.

Appendix A – AutoTableTop™ Transcript

Given the scenario and AutoTableTop™ associated settings file, this is an example transcript completed by Robert C. Rhodes on October 7th, 2024 based upon suggested play books from throughout the internet based upon the Colonial Pipeline incident. It includes the AutoTableTop™ analysis.

Facilitator: **Introduction:**

Welcome to today's Incident Response Tabletop Exercise. As the facilitator, I will guide you through the scenario and provide feedback and challenges as needed. Your role is to respond as you would in a real-world situation, make decisions, and take actions as a team. It is important to take time to discuss possibilities and actions as a team. I'm also here to help guide you, so feel free to ask me for advice at any time. This exercise is designed to test your incident response plan for a ransomware attack. Since no specific IR plan has been provided, your actions will be judged based on best practices and industry standards. The participants for this exercise are the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), and the IT Security Manager. Let's work together to ensure that Colonial Pipeline is prepared to handle a cybersecurity incident effectively.

Setting the Stage:

The current date is October 7, 2024, at 4:41 PM. Colonial Pipeline Company, founded in 1962, operates the largest refined products pipeline system in the United States. The company's network spans more than 5,500 miles, connecting refineries primarily in the Gulf Coast to markets throughout the Southern and Eastern United States. Colonial transports approximately 100 million gallons or 2.5 million barrels of fuel daily, including various grades of gasoline, diesel fuel, home heating oil, jet fuel, and fuels for the U.S. military. This critical infrastructure supplies about 45 percent of all fuel consumed on the East Coast, serving more than 50 million Americans. The pipeline system consists of two main lines and 65 stub lines, with Line 1 primarily transporting gasoline and Line 2 carrying distillates. Colonial's operations are crucial to the nation's energy supply, making it a potential target for cybersecurity threats, as demonstrated by the significant ransomware attack in May 2021.

The departments involved in this exercise include the Information Technology (IT)/Cybersecurity Team, Executive Leadership, and the Legal Department. The IT staff available includes the Incident Response Team Lead, Zion McClure, and the Cybersecurity Analyst Lead, nicknamed Tron. The environment consists of a SCADA system to monitor and control pipeline operations, a network that includes both IT and OT systems, and at least one VPN access point. The network spans the entire 5,500-mile length of the pipeline system, connecting various operational sites and includes systems for monitoring pipeline flow, pressure, and other operational data. There are multiple data centers and control rooms along the pipeline route, and the network includes business systems for billing and other corporate functions.

Scenario:

As the exercise begins, the IT Security Manager receives an alert from the network monitoring system indicating unusual activity. The SCADA system controlling pipeline flow shows unexpected changes in pressure readings. Simultaneously, an employee in the control room reports that their screen is locked with a ransomware message demanding payment in cryptocurrency. The billing system becomes inaccessible, raising concerns about the potential compromise of customer data.

Please proceed with your initial response actions.

Your Team: Activate our Incident Response Plan amended July 1, 2024.

Notify key personal - IR team lead Zion McClure and Cybersecurity Analyst Lead Tron. Also notify our executive leadership contacts in the IR plan and financial leadership responsible for the billing system.

Determine the extent to which the SCADA system was compromised.

Determine which control room systems were infected with ransomware and isolate those by taking them off the network.

Determine the billing system status and what data was breached if any. Take it off line as well.

Initiate emergency shutdown procedures on affected pipeline sections to prevent hazards.

Collect and preserve system logs for forensic review. Please show some of those as well from the control system and SCADA system.

Facilitator: As you activate your Incident Response Plan, the following actions are taken:

1. ****Notification:****

- Zion McClure, the Incident Response Team Lead, and Tron, the Cybersecurity Analyst Lead, are notified and begin coordinating the response efforts.

- Executive leadership, including the Chief Information Officer (CIO) Darrell Riekema, Chief Information Security Officer (CISO) Adam Tice, and financial leadership responsible for the billing system, are informed of the situation.

2. ****SCADA System Assessment:****

- The team begins assessing the SCADA system to determine the extent of the compromise. Initial findings indicate that the unexpected changes in pressure readings are due to unauthorized access attempts, but the core SCADA system remains operational.

3. ****Control Room Systems:****

- The control room systems infected with ransomware are identified. These systems are isolated by disconnecting them from the network to prevent further spread of the ransomware.

4. ****Billing System Status:****

- The billing system is found to be inaccessible, and initial investigations suggest that customer data may have been compromised. The system is taken offline to prevent further unauthorized access.

5. ****Emergency Shutdown Procedures:****

- Emergency shutdown procedures are initiated for the affected sections of the pipeline to prevent any potential hazards. This involves coordinating with the Pipeline Control Systems Manager and the Pipeline Operations Technology Specialist.

6. ****Log Collection and Preservation:****

- System logs from the control systems and SCADA system are collected and preserved for forensic analysis. Here are some excerpts from the logs:

****Control System Log Excerpt:****

...

[2024-10-07 16:30:12] Unauthorized access attempt detected from IP 192.168.1.45

[2024-10-07 16:31:05] Ransomware signature identified on workstation ID CR-102

[2024-10-07 16:32:47] Network isolation initiated for infected systems

...

****SCADA System Log Excerpt:****

...

[2024-10-07 16:29:50] Pressure anomaly detected on Line 1, Segment 23

[2024-10-07 16:30:15] Unauthorized command attempt blocked

[2024-10-07 16:31:30] SCADA system integrity check initiated

...

Please proceed with your next steps or any additional actions you would like to take.

Your Team: Notify the correct contacts at the Department of Homeland Security directly responsible for pipeline security. Also notify FBI and CISA.

Engage our legal department to determine what legal steps we need to complete. Also, engage our SEC counsel for any SEC mandated cybersecurity 8K disclosure statements that need to be filed.

Engage outside consulting experts on retainer, Google's Mandiant consulting firm.

Facilitator: As you proceed with the next steps in your incident response, the following actions are taken:

1. ****Notification to Authorities:****

- The Department of Homeland Security (DHS) contacts responsible for pipeline security are notified of the incident. This includes providing them with initial details of the ransomware attack and the potential impact on pipeline operations.

- The Federal Bureau of Investigation (FBI) is informed to assist with the investigation and potential criminal aspects of the attack.

- The Cybersecurity and Infrastructure Security Agency (CISA) is also notified to provide guidance and support in managing the cybersecurity incident.

2. **Engagement with Legal Department:**

- The legal department is engaged to determine the necessary legal steps to be taken in response to the incident. This includes assessing any regulatory requirements and potential liabilities.

- The SEC counsel is consulted to evaluate the need for filing a cybersecurity 8-K disclosure statement, as mandated by the Securities and Exchange Commission (SEC), to inform investors and stakeholders of the material cybersecurity event.

3. **Engagement with External Consultants:**

- Google's Mandiant consulting firm, which is on retainer, is engaged to provide expert assistance in managing the incident. Mandiant's team will work alongside your internal teams to conduct a thorough investigation, assist with containment and eradication efforts, and provide strategic guidance on recovery and remediation.

Please proceed with any additional actions or decisions you would like to make as part of the incident response process.

Your Team: Have we stopped the spread of ransomware through the affected systems?

Facilitator: At this point in the incident response process, the following actions have been taken to stop the spread of ransomware through the affected systems:

1. **Isolation of Infected Systems:**

- The control room systems identified as infected with ransomware have been isolated by disconnecting them from the network. This action is crucial in preventing the ransomware from spreading to other systems within the network.

2. **Network Segmentation:**

- The network has been segmented to ensure that the ransomware cannot propagate to other critical systems, including the SCADA system and other operational technology (OT) components.

3. **Containment Measures:**

- Additional containment measures, such as blocking unauthorized IP addresses and disabling compromised user accounts, have been implemented to further limit the spread of the ransomware.

Based on these actions, the spread of ransomware through the affected systems has been effectively contained. However, continuous monitoring and vigilance are necessary to ensure that no further infections occur. It is also important to conduct a thorough investigation to identify the initial entry point and any potential lateral movement within the network.

Please let me know if there are any additional actions you would like to take or if you have any further questions.

Your Team: Determine original compromise point and start forensics on the logs to determine extent that pipeline system can be brought back online.

Facilitator: To determine the original compromise point and assess the extent to which the pipeline system can be safely brought back online, the following actions are undertaken:

1. **Forensic Analysis of Logs:**

- The Incident Response Team, led by Zion McClure and supported by Tron, begins a detailed forensic analysis of the collected system logs. This involves examining network traffic, access logs, and system event logs to trace the initial entry point of the ransomware attack.

2. **Identifying the Compromise Point:**

- Through the forensic analysis, it is discovered that the initial compromise occurred via a compromised VPN account. The attackers exploited a lack of multifactor authentication on this account, allowing them unauthorized access to the network.

3. **Extent of Compromise:**

- The forensic team identifies that the ransomware primarily affected IT systems, including the billing system and certain control room workstations. The SCADA system and other critical OT components were not directly compromised, thanks to the swift isolation and containment measures.

4. **Assessment for Bringing Systems Back Online:**

- With the extent of the compromise understood, the team begins assessing which systems can be safely brought back online. The SCADA system, having been verified as uncompromised, is prioritized for restoration to resume pipeline operations.

- The billing system and infected control room workstations will remain offline until they are thoroughly cleaned and verified as safe.

5. **Remediation and Recovery Plan:**

- A remediation and recovery plan is developed, outlining the steps needed to restore affected systems, implement additional security measures, and prevent future incidents. This includes enhancing VPN security with multifactor authentication and conducting a comprehensive security audit.

Please proceed with any additional actions or decisions you would like to make as part of the incident response process.

Your Team: Disable VPN access points to limit potential external access. Remove all logins and begin issuing new credentials while it is still disabled.

Ensure that all systems have multi-factor authentication enabled.

Bring the SCADA system back online and monitor for normal operations.

Facilitator: As part of the ongoing incident response efforts, the following actions are taken to enhance security and begin the recovery process:

1. **Disabling VPN Access Points:**

- All VPN access points are temporarily disabled to prevent any potential external access while the incident response team works to secure the network. This action helps to eliminate any unauthorized access routes that the attackers may have used.

2. **Credential Management:**

- All existing login credentials are removed, and the process of issuing new credentials is initiated. This includes ensuring that all new credentials are strong and unique, and that they are distributed securely to authorized personnel.

3. **Enabling Multi-Factor Authentication (MFA):**

- Multi-factor authentication is enabled across all systems to provide an additional layer of security. This measure is critical in preventing unauthorized access and mitigating the risk of future compromises.

4. **Bringing the SCADA System Back Online:**

- The SCADA system is carefully brought back online after confirming that it was not directly compromised by the ransomware attack. The system is closely monitored for normal operations, with particular attention to any anomalies or unauthorized access attempts.

5. **Monitoring and Verification:**

- Continuous monitoring is implemented to ensure that all systems, including the SCADA system, are operating normally and securely. Any suspicious activity is promptly investigated to prevent further incidents.

These actions are crucial in securing the network, restoring critical operations, and preventing future attacks. Please let me know if there are any additional actions you would like to take or if you have any further questions.

Your Team: Complete control room forensics and ensure all compromised machines are isolated offline, then bring control room back online. Monitor for normal operations. Review all access logs, and show excerpts.

Facilitator: To complete the forensic analysis and ensure the secure restoration of control room operations, the following steps are undertaken:

1. **Control Room Forensics:**

- The forensic team conducts a thorough examination of all control room systems to identify any remaining traces of ransomware or other malicious activity. This includes analyzing system files, registry entries, and network connections to ensure that all compromised machines are identified.

2. **Isolation of Compromised Machines:**

- Any machines found to be compromised are kept isolated and offline. These systems will undergo a complete cleaning and re-imaging process before they can be safely reintegrated into the network.

3. **Restoration of Control Room Operations:**

- Once the forensic analysis confirms that all threats have been neutralized, the control room systems are brought back online. The team ensures that all restored systems are equipped with updated security measures, including multi-factor authentication and enhanced monitoring.

4. **Monitoring for Normal Operations:**

- The control room operations are closely monitored to ensure that all systems are functioning normally. Any anomalies or suspicious activities are immediately investigated to prevent further incidents.

5. **Review of Access Logs:**

- A comprehensive review of access logs is conducted to identify any unauthorized access attempts or unusual activities. Here are some excerpts from the access logs:

Access Log Excerpt:

...

[2024-10-07 15:45:22] Successful login from user ID: ops_admin at IP 192.168.2.10

[2024-10-07 16:00:05] Failed login attempt from IP 203.0.113.45 - user ID: unknown

[2024-10-07 16:15:30] Unauthorized access attempt blocked - user ID: compromised_user

[2024-10-07 16:40:12] Multi-factor authentication challenge issued for user ID: control_operator

...

These actions ensure that the control room is securely restored and that operations can continue safely. Please let me know if there are any additional actions you would like to take or if you have any further questions.

Your Team: Bring pipeline operations online again.

File the correct SEC mandated 8K notice of compromise. Engage our PR team and legal team to engage all clients and work with them on any effects from this incident they have received.

Facilitator: To ensure a smooth transition back to normal operations and address the necessary regulatory and client communications, the following actions are taken:

1. **Restoration of Pipeline Operations:**

- With the SCADA system and control room systems verified as secure and operational, pipeline operations are gradually brought back online. The Pipeline Control Systems Manager and Pipeline Operations Technology Specialist oversee the process to ensure that all systems are functioning correctly and safely.

2. **Filing of SEC 8-K Notice:**

- The legal team, in consultation with the SEC counsel, prepares and files the required 8-K notice. This disclosure informs investors and stakeholders of the material cybersecurity event, detailing the nature of the incident, its impact, and the steps taken to address it.

3. **Engagement with PR and Legal Teams:**

- The Public Relations (PR) team is engaged to develop a communication strategy that addresses the incident transparently and effectively. This includes preparing statements for media outlets and coordinating with the legal team to ensure that all communications are compliant with regulatory requirements.

- The legal team works closely with the PR team to engage with clients, providing them with detailed information about the incident and any potential effects they may

have experienced. This includes offering support and guidance to mitigate any disruptions caused by the incident.

These actions are critical in restoring operations, maintaining regulatory compliance, and ensuring clear communication with stakeholders and clients. Please let me know if there are any additional actions you would like to take or if you have any further questions.

Your Team: Using the forensic information gathered, create a report for upper management on the impact to our operations. Determine what the direct costs of the incident were associated with our team and outside consulting to include in the report.

Collect customer data on impact on their operations.

Using forensics, determine any data breach. Communicate with effected internal contacts and external customers.

Facilitator: To provide a comprehensive report for upper management on the impact of the incident, the following steps are taken:

1. **Forensic Report on Operational Impact:**

- A detailed forensic report is compiled, outlining the sequence of events, the systems affected, and the actions taken to contain and remediate the incident. The report highlights the initial compromise through the VPN, the spread of ransomware to IT systems, and the successful isolation of critical OT systems, including the SCADA system.

2. **Direct Costs of the Incident:**

- The direct costs associated with the incident are calculated, including internal team efforts and external consulting fees. This includes:

- Internal team overtime and resource allocation costs.

- Fees for engaging Google's Mandiant consulting firm for expert assistance.

- Costs related to system restoration, security enhancements, and communication efforts.

3. **Customer Data on Operational Impact:**

- Data is collected from customers to assess the impact on their operations. This involves reaching out to clients to gather feedback on any disruptions they experienced and providing support to mitigate those effects.

4. **Data Breach Assessment:**

- Forensic analysis confirms that the billing system was compromised, potentially exposing customer data. The extent of the data breach is determined, and affected internal contacts and external customers are promptly notified.

- Communication includes details of the breach, the data potentially exposed, and steps being taken to protect their information and prevent future incidents.

5. **Communication Strategy:**

- A communication strategy is developed in collaboration with the PR and legal teams to ensure that all stakeholders are informed transparently and effectively. This includes providing regular updates and offering resources for affected customers.

The report is prepared for upper management, providing a clear overview of the incident's impact, the response actions taken, and the financial implications. Please let me know if there are any additional actions you would like to take or if you have any further questions.

Your Team: List out some of the customers effected and their costs.

Facilitator: Based on the information gathered during the incident response and customer outreach, here are some examples of affected customers and the potential costs they incurred due to the incident:

1. **Major Airline Company:**

- **Impact:** Disruption in jet fuel supply led to flight delays and rescheduling.
- **Estimated Costs:** \$500,000 in operational disruptions and customer compensation.

2. **Regional Gas Station Chain:**

- **Impact:** Temporary fuel shortages at multiple locations resulted in lost sales.
- **Estimated Costs:** \$250,000 in lost revenue and additional logistics costs to secure alternative fuel supplies.

3. **Logistics and Transportation Company:**

- **Impact:** Delays in fuel deliveries affected fleet operations and delivery schedules.
- **Estimated Costs:** \$150,000 in operational delays and increased fuel costs.

4. **Municipal Public Works Department:**

- **Impact:** Delays in fuel deliveries impacted public transportation and emergency services.
- **Estimated Costs:** \$100,000 in operational adjustments and public communication efforts.

5. **Large Retail Chain:**

- **Impact:** Fuel supply disruptions affected distribution centers and delivery schedules.
- **Estimated Costs:** \$200,000 in logistics adjustments and potential lost sales.

These examples illustrate the range of impacts and costs experienced by different customers due to the incident. The actual costs may vary based on the specific circumstances and mitigation efforts undertaken by each customer. Please let me know if there are any additional actions you would like to take or if you have any further questions.

Your Team: List out some of the data breach items and the customers effected.

Facilitator: Based on the forensic analysis and investigation into the data breach, the following items were identified as potentially compromised, along with the affected customers:

1. **Customer Billing Information:**

- **Affected Customers:** Various commercial clients, including fuel distributors and retail chains.

- **Compromised Data:** Billing addresses, account numbers, and transaction histories.

2. **Customer Contact Details:**

- **Affected Customers:** A mix of individual and corporate clients.

- **Compromised Data:** Names, email addresses, and phone numbers.

3. **Contractual Agreements:**

- **Affected Customers:** Long-term supply contract holders, such as airlines and logistics companies.

- **Compromised Data:** Contract terms, pricing agreements, and delivery schedules.

4. **Payment Information:**

- **Affected Customers:** Primarily smaller businesses with direct billing arrangements.

- **Compromised Data:** Partial credit card information and bank account details.

5. **Operational Data:**

- **Affected Customers:** Customers with integrated supply chain management systems.

- **Compromised Data:** Order histories, delivery schedules, and inventory levels.

These data items represent the scope of the breach and the types of information that may have been exposed. Affected customers have been notified, and steps are being taken to mitigate any potential risks associated with the compromised data. Please let me know if there are any additional actions you would like to take or if you have any further questions.

Your Team: Work with legal department to submit insurance claims on our cyber risk insurance. Please detail the reports required and the steps.

Facilitator: To submit insurance claims on your cyber risk insurance, the following steps and reports are required:

1. **Engage the Legal Department:**

- Collaborate with the legal department to ensure that all necessary documentation and information are prepared for the insurance claim process. This includes understanding the specific terms and conditions of your cyber risk insurance policy.

2. **Gather Required Documentation:**

- Compile all relevant documentation related to the incident, including:

- A detailed incident report outlining the nature of the attack, the systems affected, and the timeline of events.

- Forensic analysis reports that provide evidence of the breach and the extent of the compromise.

- Financial impact assessments, including direct costs incurred for internal response efforts and external consulting services.

- Customer impact reports detailing the effects on operations and any associated costs.

3. ****Prepare a Claim Submission Report:****

- Create a comprehensive claim submission report that includes:

- An executive summary of the incident and its impact on operations.

- A breakdown of the financial losses incurred, including operational disruptions, customer compensation, and recovery efforts.

- Documentation of all mitigation and remediation actions taken to address the incident and prevent future occurrences.

- Any communication with affected customers and stakeholders, including notifications and support provided.

4. ****Coordinate with the Insurance Provider:****

- Contact your cyber risk insurance provider to initiate the claims process. Provide them with the prepared documentation and reports, and ensure that all required forms and information are submitted according to their guidelines.

5. ****Follow-Up and Communication:****

- Maintain regular communication with the insurance provider to address any questions or additional information requests. Work closely with the legal department to ensure that all aspects of the claim are handled in compliance with policy requirements.

6. ****Review and Finalize the Claim:****

- Once the claim is submitted, review any feedback or decisions from the insurance provider. Ensure that all necessary steps are taken to finalize the claim and receive the appropriate compensation for the incident.

These steps will help ensure a thorough and effective submission of your cyber risk insurance claim. Please let me know if there are any additional actions you would like to take or if you have any further questions.

Your Team: Prepare and submit. Determine an approximate recovery and what percentage of our direct and indirect costs will be recovered.

Facilitator: To prepare and submit the cyber risk insurance claim, the following actions are taken:

1. ****Preparation of Claim Submission:****

- The legal department, in collaboration with the incident response team, prepares the comprehensive claim submission report. This report includes all necessary

documentation, financial impact assessments, and evidence of the incident and response efforts.

2. **Submission to Insurance Provider:**

- The claim submission report is provided to the cyber risk insurance provider, along with any required forms and additional documentation. The submission is made in accordance with the provider's guidelines and requirements.

3. **Estimation of Recovery:**

- Based on the terms of the cyber risk insurance policy and the documentation provided, an approximate recovery amount is estimated. This includes coverage for direct costs such as internal response efforts, external consulting fees, and system restoration expenses.

4. **Percentage of Costs Recovered:**

- The estimated recovery is calculated as a percentage of the total direct and indirect costs incurred due to the incident. This includes:

- Direct costs: Internal team efforts, external consulting fees, and system restoration costs.

- Indirect costs: Customer compensation, operational disruptions, and communication efforts.

- **Approximate Recovery:** \$1,200,000

- **Percentage of Costs Recovered:** Approximately 70% of the total direct and indirect costs.

These estimates are based on the coverage limits and terms outlined in the cyber risk insurance policy. The actual recovery amount may vary depending on the insurance provider's assessment and any additional factors considered during the claims process.

Please let me know if there are any additional actions you would like to take or if you have any further questions.

Your Team: Put out an SEC 8K disclosure of insurance submission and possible recovery.

Facilitator: To issue an SEC 8-K disclosure regarding the insurance submission and potential recovery, the following steps are taken:

1. **Drafting the 8-K Disclosure:**

- The legal team, in collaboration with the SEC counsel, drafts the 8-K disclosure statement. This document provides a transparent update to investors and stakeholders about the insurance claim submission and the anticipated recovery from the cyber risk insurance policy.

2. **Content of the Disclosure:**

- The 8-K disclosure includes the following key elements:

- A brief overview of the cybersecurity incident and its impact on operations.

- Details of the insurance claim submission, including the date of submission and the insurance provider involved.

- An estimate of the potential recovery amount and the percentage of costs expected to be covered by the insurance policy.

- Any relevant information about the steps taken to mitigate the impact of the incident and enhance security measures.

3. **Review and Approval:**

- The draft disclosure is reviewed and approved by the executive leadership team and the board of directors to ensure accuracy and compliance with SEC regulations.

4. **Filing the 8-K Disclosure:**

- Once approved, the 8-K disclosure is filed with the Securities and Exchange Commission (SEC) through the EDGAR system. This ensures that the information is publicly available to investors and stakeholders.

5. **Communication with Stakeholders:**

- In addition to the SEC filing, the company communicates the disclosure to stakeholders through appropriate channels, such as investor relations updates and press releases, to ensure transparency and maintain trust.

These steps ensure that the SEC 8-K disclosure is prepared and submitted in compliance with regulatory requirements, providing stakeholders with important information about the insurance claim and potential recovery.

Please let me know if there are any additional actions you would like to take or if you have any further questions.

Your Team: Through forensics, determine possible culprits of the compromise.

Facilitator: Through the forensic investigation, the following steps are taken to identify potential culprits responsible for the compromise:

1. **Analysis of Attack Vectors:**

- The forensic team analyzes the initial attack vector, which was identified as a compromised VPN account. This analysis includes examining login attempts, IP addresses, and user activity associated with the compromised account.

2. **Review of Network Traffic:**

- Network traffic logs are scrutinized to identify any unusual patterns or connections to known malicious IP addresses. This includes tracing the origin of unauthorized access attempts and any data exfiltration activities.

3. **Threat Intelligence Correlation:**

- The forensic team correlates findings with threat intelligence data to identify any known threat actors or groups that match the tactics, techniques, and procedures (TTPs) observed in the attack. This involves consulting with cybersecurity partners and leveraging threat intelligence platforms.

4. **Indicators of Compromise (IOCs):**

- Indicators of Compromise, such as file hashes, domain names, and IP addresses, are compared against databases of known threat actors. This helps in identifying any links to previously documented cybercriminal groups.

5. **Potential Culprits:**

- Based on the forensic analysis and threat intelligence correlation, the attack exhibits characteristics similar to those used by the hacker group DarkSide. This group is known for targeting critical infrastructure with ransomware attacks, as demonstrated in the May 2021 Colonial Pipeline incident.

While the forensic investigation provides strong indicators of the potential culprits, definitive attribution in cybersecurity can be challenging due to the sophisticated methods used by threat actors to obfuscate their identities.

Please let me know if there are any additional actions you would like to take or if you have any further questions.

Your Team: Determine best practices due to our experience with this incident. Add those to our incident response plan with an update. Instigate tabletop exercises to determine our cyber posture after full recovery.

Facilitator: Based on the experience gained from this incident, the following best practices are identified and incorporated into the updated incident response plan:

1. **Enhanced Access Controls:**

- Implement multi-factor authentication (MFA) across all systems and access points, including VPNs, to prevent unauthorized access.

- Regularly review and update user access permissions to ensure that only authorized personnel have access to critical systems.

2. **Comprehensive Network Monitoring:**

- Deploy advanced network monitoring tools to detect and respond to unusual activities and potential threats in real-time.

- Establish a centralized logging system to collect and analyze logs from all network devices and systems for forensic purposes.

3. **Regular Security Audits and Penetration Testing:**

- Conduct regular security audits and penetration testing to identify and address vulnerabilities in the network and systems.

- Engage third-party cybersecurity experts to provide an unbiased assessment of the organization's security posture.

4. **Employee Security Awareness Training:**

- Implement ongoing security awareness training programs for all employees to educate them about phishing, social engineering, and other cyber threats.

- Conduct simulated phishing exercises to test and improve employee readiness to recognize and report suspicious activities.

5. **Incident Response Plan Updates:**

- Update the incident response plan to include lessons learned from the incident, ensuring that roles, responsibilities, and procedures are clearly defined.

- Establish a communication plan for timely and transparent communication with stakeholders during an incident.

6. **Regular Tabletop Exercises:**

- Schedule regular tabletop exercises to test the updated incident response plan and assess the organization's cyber posture.

- Use realistic scenarios to evaluate the effectiveness of response strategies and identify areas for improvement.

7. **Collaboration with External Partners:**

- Strengthen collaboration with external partners, including cybersecurity firms, law enforcement, and industry peers, to share threat intelligence and best practices.

By incorporating these best practices into the incident response plan and conducting regular tabletop exercises, Colonial Pipeline can enhance its cybersecurity posture and readiness to respond to future incidents effectively.

Please let me know if there are any additional actions you would like to take or if you have any further questions.

Your Team: Establish a board level expert on cybersecurity and clear reporting process from our SOC team through cyber leadership and operations. Schedule and present findings to the board and establish quarterly reporting.

Request Department of Homeland Security and Department of Energy review of response and determine what reporting must be done according to the newly instituted regulations and laws promulgated by the U.S. congress.

Facilitator: To strengthen the organization's cybersecurity governance and ensure compliance with regulatory requirements, the following actions are taken:

1. **Establishing a Board-Level Cybersecurity Expert:**

- A cybersecurity expert is appointed to the board of directors to provide strategic oversight and guidance on cybersecurity matters. This expert will play a key role in shaping the organization's cybersecurity strategy and ensuring alignment with industry best practices.

2. **Clear Reporting Process:**

- A clear and structured reporting process is established, ensuring that information flows seamlessly from the Security Operations Center (SOC) team through cyber leadership to operations and ultimately to the board. This process includes:

- Regular updates from the SOC team to the Chief Information Security Officer (CISO) and Chief Information Officer (CIO).

- Monthly cybersecurity briefings to the executive leadership team.

- Quarterly cybersecurity reports presented to the board, highlighting key findings, risks, and mitigation strategies.

3. **Presentation of Findings to the Board:**

- A comprehensive presentation is prepared for the board, detailing the findings from the recent incident, the response actions taken, and the lessons learned. This presentation includes an overview of the updated incident response plan and the best practices implemented.

4. **Quarterly Reporting:**

- A schedule is established for quarterly cybersecurity reporting to the board. These reports will provide insights into the organization's cybersecurity posture, emerging threats, and ongoing initiatives to enhance security.

5. **Request for DHS and DOE Review:**

- A formal request is submitted to the Department of Homeland Security (DHS) and the Department of Energy (DOE) for a review of the incident response. This review will provide valuable feedback on the effectiveness of the response and identify any areas for improvement.

- The organization works closely with DHS and DOE to determine the reporting requirements under newly instituted regulations and laws promulgated by the U.S. Congress. This includes ensuring compliance with any mandatory reporting and disclosure obligations.

By taking these actions, Colonial Pipeline can enhance its cybersecurity governance, ensure regulatory compliance, and maintain transparency with stakeholders.

Please let me know if there are any additional actions you would like to take or if you have any further questions.

Your Team: Complete our exercise and do an analysis.

Facilitator: ## Exercise Analysis and Report

Score: 85 out of 100

Executive 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.

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.

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.

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.

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 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.