Colonial Pipeline Scenario

For ThreatGEN AutoTableTop™

Contents

Summary

The Attack

On May 7, 2021, hackers from a group known as DarkSide gained access to Colonial Pipeline's network through a compromised VPN password[1]. The hackers exploited the lack of multifactor authentication to enter the system[1]. Once inside, they:

1) Stole approximately 100 gigabytes of data in two hours[1]
2) Infected the company's network with ransomware[1]
3) Encrypted critical data, preventing legitimate users from accessing it[1]

Improve the skills of your Crisis Management Team (CMT).
Get management buy in for security changes
Test existing incident response plans
6 BENEFITS OF RUNNING A CYBER TABLETOP EXERCISE
Build awareness of cyber risk
Improve internal and external communications
Improve response times in the event of an incident
RED GOAT

Figure 1 - What is a tabletop exercise for?

Impact and Response

The attack had far-reaching consequences:

- Colonial Pipeline halted all pipeline operations to contain the threat[1][4]
- The shutdown disrupted fuel supplies along the East Coast[1]
- President Biden declared a state of emergency[1]
- Fuel shortages and panic buying occurred in several states[4]
- Average fuel prices rose to their highest since 2014[4]

In response to the attack:

- Colonial Pipeline paid a ransom of nearly $4.4 million in Bitcoin within hours[2][4]
- The company engaged third-party cybersecurity experts to investigate and respond[2]
- The U.S. government, including the FBI, CISA, and NSA, assisted in the response[2]

Aftermath and Lessons Learned

The incident highlighted several important cybersecurity lessons:

1) The critical need to protect infrastructure from cyber threats[1]
2) The importance of basic security measures like multifactor authentication[1]
3) The vulnerabilities associated with VPN systems and password security[3]
4) The potential for significant economic and societal disruption from cyberattacks on critical infrastructure[1][4]

The Colonial Pipeline attack served as a wake-up call for organizations across all industries, emphasizing the need for robust cybersecurity measures and incident response plans[3].

Citations

[1] https://insurica.com/blog/colonial-pipeline-ransomware-attack

[2] https://www.msspalert.com/news/colonial-pipeline-investigation

[3] https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack

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

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

[6] https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[7] https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

[8] https://www.wallix.com/what-happened-in-the-colonial-pipeline-ransomware-attack-2/

AutoTableTop Settings

Threat Scenario

The Colonial Pipeline cybersecurity incident in May 2021 involved a sophisticated ransomware attack by the hacker group DarkSide. The attackers gained access to Colonial Pipeline's network through a compromised VPN password, exploiting the lack of multifactor authentication[1]. Once inside, they stole approximately 100 gigabytes of data and infected the company's network with ransomware, encrypting critical information[1]. This attack forced Colonial Pipeline, the largest refined oil products pipeline in the United States, to halt all operations, disrupting fuel supplies along the East Coast and causing widespread economic impacts[1]. The incident highlighted the vulnerability of critical infrastructure to cyber threats and the potential for significant societal disruption from such attacks[1][3].

Citations:

[1] https://insurica.com/blog/colonial-pipeline-ransomware-attack/

[2] https://www.msspalert.com/news/colonial-pipeline-investigation

[3] https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic

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

[5] https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack

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

[7] https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[8] https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

Company

Colonial Pipeline

Company Information

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[1][2]. 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[1]. This critical infrastructure supplies about 45 percent of all fuel consumed on the East Coast, serving more than 50 million Americans[1]. The pipeline system consists of two main lines and 65 stub lines, with Line 1 primarily transporting gasoline and Line 2 carrying distillates[3]. 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[5].

Citations:

[1] https://www.colpipe.com/about-us/faqs

[2] https://www.colpipe.com/about-us/our-company

[3] https://www.colpipe.com/news/in-the-news/colonial-pipeline-101-know-colonial

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

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

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

[7] https://www.colpipe.com

[8] https://www.colpipe.com/about-us

Department

Based on best practices for tabletop exercises, we recommend including 5-7 key departments in a live tabletop exercise for the Colonial Pipeline scenario. This number allows for comprehensive coverage of critical areas while keeping the exercise manageable and focused. The most appropriate departments to include would be:

1) Information Technology (IT)/Cybersecurity Team
2) Operations/Pipeline Management
3) Executive Leadership
4) Legal Department
5) Public Relations/Communications

If resources allow, you could also consider adding:

6) Human Resources
7) Finance/Accounting

This selection ensures representation from technical, operational, and business aspects of incident response. It allows for a well-rounded approach without overwhelming participants or diluting the exercise's effectiveness[1][4].

Including these departments enables the exercise to cover key areas such as:

- Technical response and investigation
- Operational impact and mitigation
- High-level decision making
- Legal and regulatory considerations
- Internal and external communications
- Financial implications

Remember, the goal is to create a collaborative environment where participants can discuss their roles and responses effectively[2]. Starting with a core group of 5-7 departments provides a solid foundation for a productive tabletop exercise, allowing for meaningful interaction and decision-making processes to be tested.

Citations:

[1] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

[2] https://www.csoonline.com/article/570871/tabletop-exercises-explained-definition-examples-and-objectives.html

[3] https://www.calhospitalprepare.org/post/what-difference-between-tabletop-exercise-drill-functional-exercise-and-full-scale-exercise

[4] https://www.police1.com/police-training/articles/virtual-tabletop-exercise-public-safety-leaders-demonstrate-importance-of-interagency-training-mlzzUdW2rX2EMHXW/

[5] https://campusguard.com/post/cybersecurity-tabletop-exercises-for-leadership-teams/

[6] https://www.sans.org/blog/top-5-ics-incident-response-tabletops-and-how-to-run-them/

[7] https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

[8] https://www.reddit.com/r/k12sysadmin/comments/1095zud/cybersecurity_tabletop_exercises/

Exercise Objectives

Here are some examples of effective tabletop exercise objectives:

1) Assess the communication plan during a data security breach.
2) Practice resource allocation and decision-making during a natural disaster.
3) Identify gaps in the business continuity plan following a power outage.
4) Evaluate the effectiveness of the evacuation plan in response to a fire alarm.
5) Improve collaboration among departments in a product recall scenario.
6) **Test the incident response plan for a ransomware attack.**
7) Evaluate the organization's ability to coordinate with external stakeholders during a crisis.
8) Assess the team's readiness and knowledge in responding to a specific emergency scenario.
9) Test new or updated emergency procedures.
10) Improve response time and effectiveness compared to previous tabletop exercise performances.

When crafting objectives for a tabletop exercise, it's important to make them SMART (Specific, Measurable, Achievable, Relevant, and Time-bound). The objectives should be clearly defined and align with the organization's goals for emergency preparedness and response. They should also be tailored to the specific scenario being simulated and focus on key aspects of the response plan that need evaluation or improvement.

List of relevant sources:

[1] https://www.alertmedia.com/blog/tabletop-exercises/

[2] https://www.ravemobilesafety.com/blog/tips-conducting-effective-tabletop-exercise/

[3] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

[4] https://securityscorecard.com/blog/what-are-tabletop-exercises/

[5] https://nexightgroup.com/9-steps-to-design-a-powerful-tabletop-exercise/

[6] https://www.csoonline.com/article/570871/tabletop-exercises-explained-definition-examples-and-objectives.html

[7] https://www.alertmedia.com/blog/tabletop-exercise-scenarios/

[8] https://www.csoonline.com/article/518982/tabletop-exercise-scenarios.html

Participants

ThreatGEN is not aware of the exact company positions within Colonial Pipeline that participated In the handling of the incident; however, based on the recommended departments for a tabletop exercise in a similar setting, here's a list of possible individual participants' titles:

- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- IT Security Manager
- Network Administrator
- Chief Operating Officer (COO)
- Pipeline Operations Manager
- Control Room Supervisor
- Chief Executive Officer (CEO)
- Chief Financial Officer (CFO)
- General Counsel
- Compliance Officer
- Public Relations Director
- Corporate Communications Manager
- Human Resources Director
- Risk Management Officer
- Emergency Response Coordinator
- Business Continuity Manager
- Incident Response Team Lead
- Cybersecurity Analyst
- Digital Forensics Specialist
- Customer Service Manager
- Supply Chain Manager
- Environmental Health and Safety Manager
- Government Relations Director
- Board Member (if applicable)

This list covers a range of roles across different departments, ensuring a comprehensive representation of key decision-makers and subject matter experts. Depending on the specific goals of your exercise and the size of your organization, you may choose to include all or a subset of these roles.

IT Staff

Here's a list of high-level roles in the IT department that could be included:

1) Chief Information Officer (CIO)
2) Chief Information Security Officer (CISO)
3) Chief Technology Officer (CTO)
4) IT Director
5) IT Security Manager
6) Network Architecture Manager
7) Infrastructure Manager
8) Applications Manager
9) Database Manager
10) IT Operations Manager
11) IT Project Manager
12) Incident Response Team Lead
13) Cybersecurity Analyst Lead
14) Cloud Services Manager
15) Data Center Manager

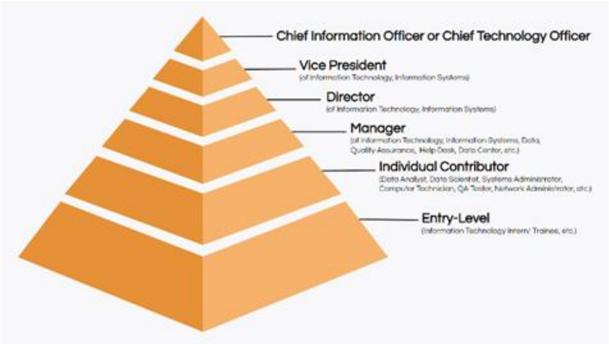

Chief Information Officer or Chief Technology Officer
Vice President
(of Information Technology, Information Systems)
Director
(of Information Technology, Information Systems)
Manager
(of Information Technology, Information Systems, Data, Quality Assurance, Help Desk, Data Center, etc.)
Individual Contributor
(Data Analyst, Data Scientist, Systems Administrator, Computer Technician, QA Tester, Network Administrator, etc.)
Entry-Level
(Information Technology Intern/ Trainee, etc.)

Figure 2 - General IT staff involved

These roles represent key decision-makers and leaders within the IT department who would likely be involved in responding to a major cybersecurity incident. They cover various aspects of IT operations, security, infrastructure, and management that would be crucial in addressing a ransomware attack or similar threat to critical systems.

List of relevant sources:

[1] https://www.coursera.org/articles/highest-paying-it-jobs

[2] https://www.multiverse.io/en-US/blog/highest-paying-tech-jobs

[3] https://www.cio.com/article/474960/highest-paying-it-jobs.html

[4] https://www.roberthalf.com/us/en/insights/career-development/highest-paying-it-jobs

[5] https://www.simplilearn.com/highest-paying-tech-jobs-article

[6]https://www.reddit.com/r/ITCareerQuestions/comments/134aq8l/what_are_the_highest_paying_jobs_in_it_you_have/

[7] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

[8] https://www.congress.gov/event/117th-congress/house-event/LC67088/text

OT Staff (If Applicable)

Here is a general list of OT (Operational Technology) staff that might be found in many companies, and then suggested specific roles that were likely relevant for Colonial Pipeline.

General OT staff for any company:

1) Chief Information Officer (CIO)
2) Chief Technology Officer (CTO)
3) OT Manager
4) OT Security Manager
5) Control Systems Engineer
6) SCADA Engineer
7) Industrial Control Systems (ICS) Specialist
8) Automation Engineer
9) Network Engineer (OT focus)
10) OT Security Analyst
11) OT Systems Administrator
12) OT Project Manager

Specific OT staff that could have taken part in the handling of the Colonial Pipeline incident:

1) Pipeline Control Systems Manager
2) SCADA Systems Engineer
3) Pipeline Operations Technology Specialist
4) Industrial Cybersecurity Manager
5) OT/IT Integration Specialist
6) Pipeline Automation Engineer
7) OT Network Security Analyst
8) Pipeline Monitoring Systems Administrator
9) Industrial Control Systems (ICS) Security Specialist
10) OT Compliance Officer
11) Pipeline Data Analytics Specialist
12) OT Incident Response Coordinator

These roles would be tailored to Colonial Pipeline's specific needs as a major oil pipeline operator, focusing on the security, efficiency, and reliability of their pipeline control and monitoring systems.

List of relevant sources:

[1] https://www.dmu.edu/ot/faculty-and-staff-3/

[2] https://otpotential.com/occupational-therapy-directory

[3] https://www.nbcot.org/-/media/PDFs/State_Contact_List.pdf

[4] https://www.gblions.org/jshs/about/staff-directory

[5] https://www.congress.gov/event/117th-congress/house-event/LC67088/text

[6] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

[7] https://www.mghihp.edu/health-rehabilitation-sciences/departments-programs/occupational-therapy

[8] https://campusguard.com/post/cybersecurity-tabletop-exercises-for-leadership-teams/

Cybersecurity Staff

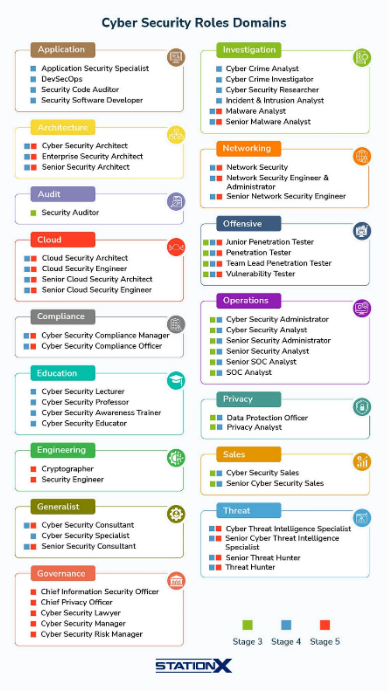
Here is a list of general cybersecurity roles and suggestions of some specific roles that would likely be relevant for Colonial Pipeline:

General cybersecurity roles

1) Chief Information Security Officer (CISO)
2) Information Security Manager
3) Cybersecurity Analyst
4) Incident Response Specialist
5) Penetration Tester/Ethical Hacker
6) Security Operations Center (SOC) Analyst
7) Network Security Engineer
8) Application Security Specialist
9) Cloud Security Architect
10) Compliance Specialist

Specific cybersecurity roles likely relevant for Colonial Pipeline:

1) Pipeline Cybersecurity Manager
2) Industrial Control Systems (ICS) Security Specialist
3) SCADA Security Engineer
4) OT/IT Security Integration Specialist
5) Cybersecurity Incident Response Coordinator
6) Critical Infrastructure Protection Analyst
7) Ransomware Prevention Specialist
8) Supply Chain Security Analyst
9) Cyber Threat Intelligence Analyst (focused on energy sector threats)
10) Security Awareness Training Coordinator



Cyber Security Roles Domains

Application
- 🟦 Application Security Specialist
- 🟦 DevSecOps
- 🟦 Security Code Auditor
- 🟦 Security Software Developer

Architecture
- 🟦🟥 Cyber Security Architect
- 🟦🟥 Enterprise Security Architect
- 🟦🟥 Senior Security Architect

Audit
- 🟩 Security Auditor

Cloud
- 🟦🟥 Cloud Security Architect
- 🟦🟥 Cloud Security Engineer
- 🟦🟥 Senior Cloud Security Architect
- 🟦🟥 Senior Cloud Security Engineer

Compliance
- 🟦🟥 Cyber Security Compliance Manager
- 🟦🟥 Cyber Security Compliance Officer

Education
- 🟦 Cyber Security Lecturer
- 🟦 Cyber Security Professor
- 🟦 Cyber Security Awareness Trainer
- 🟦 Cyber Security Educator

Engineering
- 🟥 Cryptographer
- 🟥 Security Engineer

Generalist
- 🟦🟥 Cyber Security Consultant
- 🟦 Cyber Security Specialist
- 🟦🟥 Senior Security Consultant

Governance
- 🟥 Chief Information Security Officer
- 🟥 Chief Privacy Officer
- 🟥 Cyber Security Lawyer
- 🟥 Cyber Security Manager
- 🟥 Cyber Security Risk Manager

Investigation
- 🟦 Cyber Crime Analyst
- 🟦 Cyber Crime Investigator
- 🟦 Cyber Security Researcher
- 🟦 Incident & Intrusion Analyst
- 🟦🟥 Malware Analyst
- 🟦🟥 Senior Malware Analyst

Networking
- 🟦🟥 Network Security
- 🟦🟥 Network Security Engineer & Administrator
- 🟦🟥 Senior Network Security Engineer

Offensive
- 🟩🟦🟥 Junior Penetration Tester
- 🟩🟦🟥 Penetration Tester
- 🟩🟦🟥 Team Lead Penetration Tester
- 🟩🟦🟥 Vulnerability Tester

Operations
- 🟩🟦 Cyber Security Administrator
- 🟩🟦 Cyber Security Analyst
- 🟩🟦 Senior Security Administrator
- 🟩🟦 Senior Security Analyst
- 🟩🟦 Senior SOC Analyst
- 🟩🟦 SOC Analyst

Privacy
- 🟩🟦 Data Protection Officer
- 🟩🟦 Privacy Analyst

Sales
- 🟩🟦 Cyber Security Sales
- 🟩🟦 Senior Cyber Security Sales

Threat
- 🟦🟥 Cyber Threat Intelligence Specialist
- 🟦🟥 Senior Cyber Threat Intelligence Specialist
- 🟦🟥 Senior Threat Hunter
- 🟦🟥 Threat Hunter

🟩 Stage 3 🟦 Stage 4 🟥 Stage 5

STATIONX

Figure 3 - General roles in cybersecurity

These specific roles would be tailored to address the unique cybersecurity challenges faced by a major oil pipeline operator like Colonial Pipeline. They would focus on protecting industrial control systems, SCADA networks, and the critical infrastructure that the company operates, as well as addressing threats specific to the energy sector.

List of relevant sources:

[1] https://www.techtarget.com/whatis/feature/5-top-cybersecurity-careers

[2] https://www.congress.gov/event/117th-congress/house-event/LC67088/text

[3] https://www.coursera.org/articles/cybersecurity-jobs

[4] https://plextrac.com/blog/12-examples-of-cybersecurity-jobs/

[5] https://www.varonis.com/blog/working-in-cybersecurity

[6] https://www.simplilearn.com/it-security-professionals-key-roles-responsibilities-article

[7] https://www.cio.com/article/474960/highest-paying-it-jobs.html

[8] https://campusguard.com/post/cybersecurity-tabletop-exercises-for-leadership-teams/

Leadership Staff

Based on publicly available sources of information, here are the key leadership staff associated with Colonial Pipeline:

- Melanie Little - President and Chief Executive Officer (as of January 2, 2023)
- Joseph A. Blount - Former CEO (until end of 2022)
- Clay Miller - Vice President and Chief Financial Officer
- Adam Tice - Chief Information Security Officer
- Darrell Riekena - Chief Information Officer and Senior Vice President
- Angie Kolar - Vice President Operations Services & Chief Risk Officer
- Marie Mouchet - VP & CIO
- Daniel 'Dan' Gordon - VP/Chief Commercial Officer
- Jamie Chapman - Vice President (role not specified)
- Rodney L. Gray - Vice President and Chief Financial Officer (as of January 27, 2024)

It's worth noting that some of this information may be outdated, as leadership changes have occurred over time. For instance, Melanie Little succeeded Joseph A. Blount as President and CEO, and Rodney L. Gray was announced as the new VP and CFO in a more recent press release.

List of relevant sources:

[1] https://www.zippia.com/colonial-pipeline-careers-19622/executives/

[2] https://rocketreach.co/colonial-pipeline-company-management_b5c624f3f42e0caa

[3] https://www.colpipe.com/news/press-releases/colonial-names-rodney-l-gray-vice-president-chief-finanical-officer

[4] https://www.colpipe.com/about-us/our-company

[5] https://www.colpipe.com/news/press-releases/melanie-little-named-president-ceo-of-colonial-pipeline-company

[6] https://www.congress.gov/event/117th-congress/house-event/LC67088/text

[7] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

[8] https://www.gblions.org/jshs/about/staff-directory

Network Environment

We don't have detailed information about Colonial Pipeline's specific computer network design or exact amount of equipment. The publicly available information does not provide that level of technical detail about their internal systems. However, based on the general information available, we can infer a few things about Colonial Pipeline's network:

1) They likely used a SCADA (Supervisory Control and Data Acquisition) system to monitor and control the pipeline operations.
2) The network included both IT (Information Technology) and OT (Operational Technology) systems. The ransomware attack primarily affected the IT systems.
3) There was at least one VPN (Virtual Private Network) access point, as the attackers gained initial access through an outdated VPN account.
4) The network spanned the entire 5,500 mile length of the pipeline system, connecting various operational sites.
5) It included systems for monitoring pipeline flow, pressure, and other operational data.
6) There were likely multiple data centers and control rooms along the pipeline route.
7) The network included business systems for billing and other corporate functions.

Without access to Colonial Pipeline's internal documentation or network diagrams, it's not possible to provide specific numbers of servers, workstations, or other network equipment. Such detailed information about critical infrastructure is typically not made public due to security concerns.

List of relevant sources:

[1] https://www.congress.gov/event/117th-congress/house-event/LC67088/text

[2] https://www.colpipe.com/safe-operations/system-safety-and-integrity

[3] https://mwi.westpoint.edu/the-colonial-pipeline-hack-shows-we-need-a-better-federal-cybersecurity-ecosystem/

[4] https://www.colpipe.com

[5] https://www.cybersecuritydive.com/news/post-colonial-pipeline-attack/623859/

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

[7] https://www.colpipe.com/about-us/our-company

[8] https://www.colpipe.com/safe-operations/emergency-preparedness

Injects

Here are some general injects for a cybersecurity tabletop exercise, followed by specific injects tailored to a Colonial Pipeline scenario:

General cybersecurity tabletop exercise injects

- An employee reports receiving a suspicious email with an attachment.

- The IT team detects unusual network traffic from a server.
- A critical system suddenly becomes unresponsive.
- An external partner reports a potential data breach involving shared information.
- Social media posts claim to have accessed sensitive company data.
- Ransomware messages appear on multiple workstations.
- A phishing campaign targets executives with fake login pages.
- An insider threat is suspected based on unusual data access patterns.

Specific injects for a Colonial Pipeline tabletop exercise

1) The SCADA system controlling pipeline flow shows unexpected changes in pressure readings.
2) An employee in the control room reports their screen is locked with a ransomware message.
3) The billing system becomes inaccessible, potentially compromising customer data.
4) Unusual remote access attempts are detected on the VPN used for pipeline monitoring.
5) A threat actor claims on a dark web forum to have infiltrated Colonial Pipeline's network.
6) Multiple pipeline monitoring stations lose connectivity simultaneously.
7) An employee reports receiving a spear-phishing email impersonating the CEO, Joseph Blount.
8) The OT network firewall logs show attempts to access industrial control systems from the IT network.
9) A third-party vendor with access to Colonial's systems reports a potential compromise of their own network.
10) Media outlets begin reporting on potential fuel shortages due to a suspected cyberattack on Colonial Pipeline.

These injects are designed to test the incident response capabilities of various departments, including IT/cybersecurity, operations, executive leadership, legal, and public relations. They simulate the escalating nature of a cyber incident and require participants to make decisions, communicate effectively, and manage both technical and business aspects of the crisis.

List of relevant sources:

[1] https://law.shu.edu/documents/questions-mb1018.pdf

[2] https://www.reddit.com/r/k12sysadmin/comments/1095zud/cybersecurity_tabletop_exercises/

[3] https://www.linkedin.com/pulse/how-run-cyber-exercise-part-7-injects-chris-baars-cism-crisc

[4] https://www.mandiant.com/sites/default/files/2021-09/ds-tabletop-exercise-000005-2.pdf

[5] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf

[6] https://rems.ed.gov/docs/CybersecurityTabletop_508C.pdf

[7] https://www.reddit.com/r/cybersecurity/comments/1eeq2jy/tabletop_exercises_resources_examples/

[8] https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages