Case

Out of Gas: A Deep Dive Into the Colonial Pipeline Cyberattack

Less information

Case

Teaching Notes

Abstract

In May 2021, the United States received an abrupt education about the Colonial Pipeline after a cyberattack caused a gas shortage along the East Coast, leading to a state of emergency. The cyberattack on the Colonial Pipeline caused many businesses, residents, and airports to enter a crisis mode and scramble to find alternative fuel sources and adjust plans during the beginning of the summer season and reopening following the COVID-19 pandemic shut downs.

This case demonstrates many concepts of public relations and business communication in practice, including crisis communication, internal communication, employee relations, and security. Through an examination and understanding of what happened during the Colonial Pipeline cyberattack, we can learn how to be more prepared for a crisis and how to effectively respond when one inevitably occurs.

Case

Learning Outcomes

By the end of this case, students should be able to:

- explain the importance of having a comprehensive crisis plan;
- analyze how organizations interact with government rules and regulations;
- evaluate the impact of business operations on the global marketplace;
- cite examples of the role of public relations within organizations and external stakeholders.

The History of the Colonial Pipeline

The Colonial pipeline stretches from Houston, Texas to New Jersey. It is the largest pipeline in the United States and delivers an average of 100,000,000 U.S. gallons of gas, oil, fuel, and other petroleum daily (Colonial Pipeline, 2021). This pipeline provides nearly half of the gas and fuel consumed on the east coast of the United States. The Colonial Pipeline first began operating in 1965 and remains operational today, at least until it was hacked in the spring of 2021, briefly ceasing operations and causing a major gas shortage up and down the southern east coast of the United States.

The Colonial pipeline is owned by five different groups, Koch Industries being the leader with a 28% ownership stake. It is operated by the Colonial Pipeline Group (CPG), which is headquartered in Alpharetta, Georgia (Colonial Pipeline, 2021). Over the past 60 years of operations, the Colonial Pipeline Group has been no stranger to a crisis. The recent cyberattack in 2021, while unique and different from previous issues, was not the first time CPG was thrust into the national spotlight for unfavorable reasons.

Throughout the inception and development of the pipeline, CPG could be perceived as innovative and praised for the rapid expansion of fuel dissemination. For instance, CPG designed a unique hydraulic system in 1963 to combat the issue of gas intermixing, rendering it unsafe for use. The same year, CPG overcame Hurricane Cindy and continued to expand the product market by reaching North Carolina and Virginia, before becoming fully operational.

Within two years of reaching full operations, CPG began to expand its capacity in order to

for people and eventually doubled the pipeline's capacity through adding a parallel, second line. By 1990, the pipeline had reached record volumes, completed necessary updates, and greatly expanded its reach since inception. While the development record of the pipeline is impressive, it is not without some flaws and hiccups.

CPG's Environmental Record

In 1970, the pipeline's first leak was detected in Maryland, following resident reports of gasoline odors and leakage, and a non-fatal explosion and fire. More than 20 years later, in 1991, a second spill occurred when part of the pipeline ruptured in South Carolina. This resulted in the loss of about 500,000 gallons of diesel fuel which flowed into a neighboring creek. The leak resulted in huge environmental damage and forced some residents in South Carolina to seek an alternative water source (National Transportation and Safety Board, 1972).

Less than two years later, there was another pipe rupture in Virginia, near Washington DC, that created a diesel geyser and ultimately polluted the Potomac River. There were issues again in 1994, 1996, 1997, and 1999, all of which caused environmental and residential damage and cost CPG a significant amount of money in repairs and settlements.

The new century, however, brought CPG some welcome praise and growth. CPG made business acquisitions that allowed for increased capacity and was recognized by the American Petroleum Institute for its safety and environmental record, despite the previous spills. Following the terror attacks of September 11, 2001, CPG made improvements to its security, which later received federal praise, and topped off the year with a production record. However, spills continued throughout the south-eastern United States, and the Environmental Protection Agency did not join in the praise of CPG, citing the company for gross negligence in many of the spills previously mentioned. This ended up costing CPG a civil penalty of USD 34 million with a promise to upgrade environmental protection on the pipeline to the tune of an additional USD 30 million (Environmental Protection Agency, 2003; Parker, 2002).

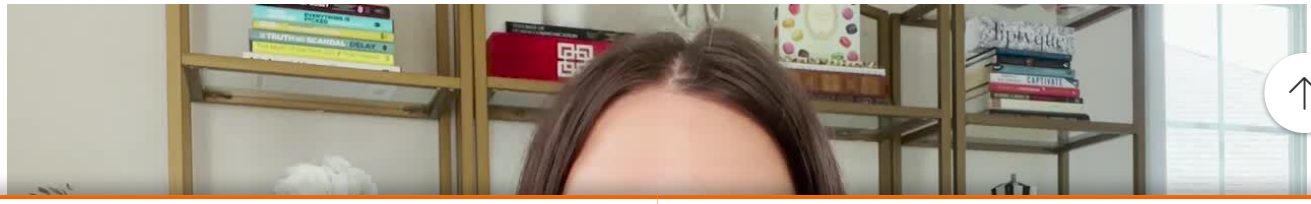
2021 Cyberattack

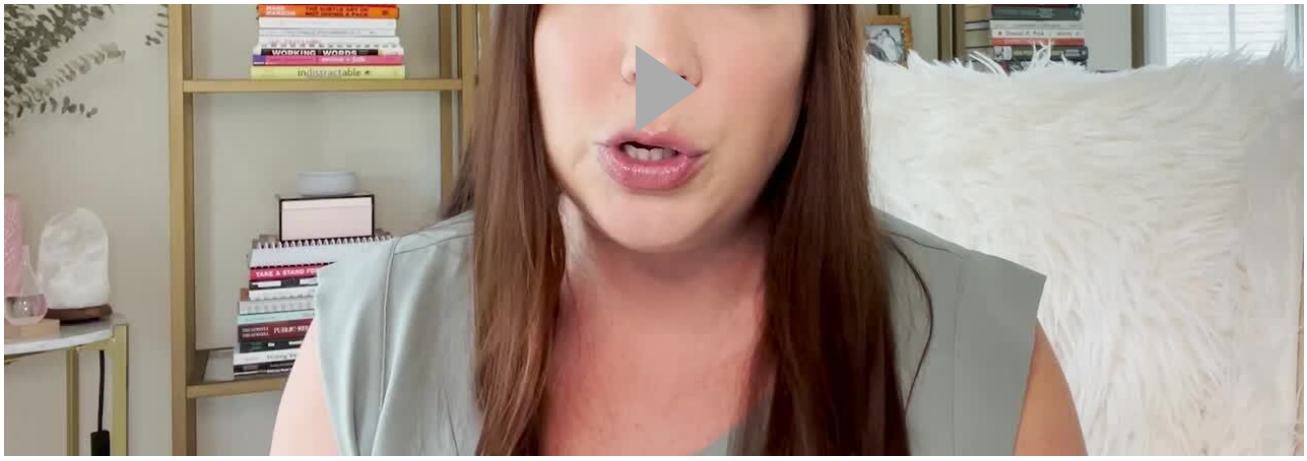
In the pipeline's history, it had only paused all service operations once, pending a year 2000 problem-related power outage that never materialized. Although some of the previous spills and natural disasters, such as hurricanes, had caused the pipeline to reduce operations, it was not until 2021 that the pipeline shut down for a considerable amount of time. In this case, operations restarted after a six-day shutdown. However, it took an additional three days for the pipeline to reach full operating capacity after being restarted.

On May 7, 2021, CPG was the victim of a ransomware cyberattack on the computer system and equipment that manages and operates the pipeline. Due to the attack and security breach, CPG had to halt all operations to ensure the attack was over and to determine how to move forward. CPG worked with the Federal Bureau of Investigation and also paid the requested ransom of 75 bitcoin worth approximately USD 4.4 million. Upon paying the ransom, the hackers restored CPG's network, but CPG continued to operate at a slower and reduced capacity, causing a regional emergency and fuel shortage throughout the east coast of the United States (Krauss, 2021).

The hack is believed to have been caused by one compromised password, not several, that was leaked during a previous data breach. However, the leaked password was for a virtual private network (VPN) that was no longer in use, but that did provide access to Colonial's computer network. Around 5 a.m. on May 7, 2021, a CPG employee saw a ransom note appear on a computer and by 6:10 a.m., the entire pipeline had been shut down. According to CEO Joseph Blount, "We had no choice at that point. It was absolutely the right thing to do. At that time, we had no idea who was attacking us or what their motives were." Blount's decision to pay the ransom has been controversial in the public forum and was questioned during a congressional hearing in June 2021 (Gregg, 2021; Krauss, 2021).

Video 1. Communicating the Decision





Transcript

00:00 [MUSIC PLAYING]

00:09 STEPHANIE SMITH: Hi, I'm Stephanie Smith. I'm an associate professor of public relations in Virginia Tech's School of Communication. My research focuses on job searching and employee retention among the entry level workforce, and recruiting a multi-generational workforce as well. Joseph Blount's description of his decision making process to pay the ransom following the cyber attack came across as very reactive and

Download transcript.

During the investigation, it was determined that the hack only affected the billing technology. However, because no one could be accurately billed during this time, the shut-down helped avoid unnecessary costs and billing issues. To be clear, the hack did not compromise the operation of the pipeline, nor was there any physical damage to the pipeline. Unfortunately, despite paying the ransom and beginning an investigation within a few hours of the breach, a crisis had erupted throughout the eastern portion of the United States (Krauss, 2021).

The Timeline and Response

Two days after the attack on May 9, President Joe Biden declared a state of emergency. This removed limits on the transportation of fuels by road to help alleviate any shortages. The next day, Georgia's Governor, Brian Kemp, declared a state of emergency and waived state tax collection on motor fuels. On May 12, the U.S. Transportation Secretary and the U.S. Energy Secretary cautioned against fuel-hoarding and referred to the crisis as a

Due to fuel shortages resulting from the shut-down, major airports such as Charlotte Douglas International and Hartsfield-Jackson Atlanta International Airport had to use other fuel suppliers and change flight schedules. Some other regional airports were similarly affected (Krauss, 2021).

By the fourth day of the shutdown, fuel shortages began occurring at gas stations across the south and Mid-Atlantic states in Alabama, Florida, Georgia, and North and South Carolina, as well as Virginia. In Charlotte, North Carolina, 71% of gas stations were out of fuel. In Washington DC, 87% of stations had no fuel for customers. The shutdown not only caused outages and public panic, but also gas prices rose to the highest price since 2014, at more than USD 3 per gallon. While the pipeline was fully operational again by May 15, it was not until after May 18 that gas stations could resume providing fuel to customers without a shortage.

The investigation of the pipeline attack continued after operations were restored and as of early June, about half of the ransom payment had been recovered. Despite early speculation that the Russian government was responsible for the attack, it was determined that the Russian group known as *DarkSide* was in fact responsible.

On June 8, 2021, Joseph Blount testified about the hack during a congressional hearing. He began his testimony with an apology, stating: “We are deeply sorry for the impact this attack had but are heartened by the resilience of our country and our company.” Although he apologized, he was defensive regarding the fact that the entire network was compromised by one password leak, which critics argue was the result of irresponsible and insecure business practice. Blount argued: “It was a complicated password…I want to be clear on that…it was not a ‘colonial 123’ type password.” He also added that moving forward, CPG has instituted multi-factor authentication and is more compliant with cybersecurity regulations, stating: “Colonial Pipeline can—and we will—continue investing in cybersecurity and strengthening our systems.” (Englund & Nakashima, 2021).

Video 2. Protecting the Colonial Pipeline Brand

Transcript

00:00 [MUSIC PLAYING]

00:10 SPEAKER: Blount attempted to protect the Colonial Pipeline brand during his testimony by clearly explaining that this was not just a cause of some one employee's irresponsibility. He made it clear that this could happen to nearly any organization. And as we've seen in other instances, it has happened to other organizations. However, he went out of his way not to place any blame onto his employees, and he also took

Download transcript.

The Biden Administration later mandated the reporting of cyberattacks like this to federal authorities following this incident to help avoid a national emergency.

While CPG lacked some cybersecurity, this incident brought to light the limits that any company can face when trying to prevent and respond to cyberattacks and the government agrees that further discussions and policies need to be explored. However, during the hearing Blount did admit to CPG's lack of inclusion of a ransom or cyberattack in its disaster preparedness plan (Englund & Nakashima, 2021). The hack, therefore, serves as a stark lesson to other companies to prepare for more than natural disasters and operational failures, which had previously been all that CPG had faced.

Video 3. Crisis Communication

Transcript

00:00 [MUSIC PLAYING]

00:09 STEPHANIE SMITH: Companies need a crisis communication strategy because they need to be prepared for anything to happen. A crisis is always a surprise, meaning that you can never predict exactly when it's going to happen. However, you can be prepared in your communication and know exactly what you're going to do and who is going to say what and where they're going to say it and when they're going to say it as soon as

Download transcript.

Discussion Questions

1. How could the Colonial Pipeline Group have better prepared for this crisis?
2. Was Blount's choice within the Public Relations Society of America (PRSA) Code of Ethics? Why and how?
3. What public relations/communication theories do you see present in this case?
4. What can other organizations learn from this case to improve their own business operations and communication strategies?
5. What responsibility do you think the federal government has in issues of cybersecurity for business organizations?

Further Reading

Congressional hearing: www.c-span.org/video/?512332-1/colonial-pipeline-ceo-joseph-blount-testifies-house-homeland-security-committee

JBS Meat Supply Hack: www.washingtonpost.com/business/2021/06/01/jbs-cyberattack-meat-supply-chain/

PRSA Code of Ethics: www.prsa.org/about/prsa-code-of-ethics

References

Colonial Pipeline (2021). *About Us*. www.colpipe.com/about-us/our-company

Englund, W. , & Nakashima, E. (2021, December 12). Panic buying strikes Southeastern United States as shuttered pipeline resumes operations. *The Washington Post*. https://www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/

Environmental Protection Agency. (2003). Enforcement: Colonial Pipeline Clean Water Act settlement. Retrieved from: www.epa.gov/enforcement/colonial-pipeline-company-clean-water-act-settlement

Gregg, A. (2021, June 8). CEO defends Colonial Pipeline's ransomware response during Senate hearing. *The Washington Post*. www.washingtonpost.com/business/2021/06/08/colonial-pipeline-ceo-blount-congress/

Krauss, C. (2021, May 10). How the Colonial Pipeline became a vital artery for fuel. *The New York Times*. www.nytimes.com/2021/05/10/business/colonial-pipeline-ransomware.html

National Transportation and Safety Board. (1972). https://web.archive.org/web/20121009215739/https://www.ntsb.gov/doclib/recletters/1972/P72_1_7.pdf

Parker, B. (2002). *Colonial Pipeline: Courage, Passion, Commitment*. Parker Hood.

Read next

Tools On this page

More like this

SAGE Recommends

We found other relevant content for you on other SAGE platforms.

Also from SAGE Publishing

CQ Press Library

American political resources

Data Planet

A universe of data

Lean Library

Increase the visibility of your library

SAGE Campus

Online skills and methods courses

SAGE Journals

World-class research journals

SAGE Research Methods

The ultimate methods library

About

About SAGE Knowledge

About SAGE Publishing

Accessibility

Terms of use

CCPA – Do Not Sell My Personal Information

CCPA

Privacy policy

Information for

Authors

Instructors

Librarians

Students and researchers

Trial Login

Frequently Asked Questions

Stay in touch

Contact us