INSTRUCTOR ALTON

Colonial Pipeline Case Study

A Failure in IT Risk Management

Background Information

On May 7, 2021, Colonial Pipeline, one of the largest oil pipelines in the United States that delivers roughly 45% of all fuel consumed on the east coast, fell victim to a ransomware attack that affected their billing and accounting software.

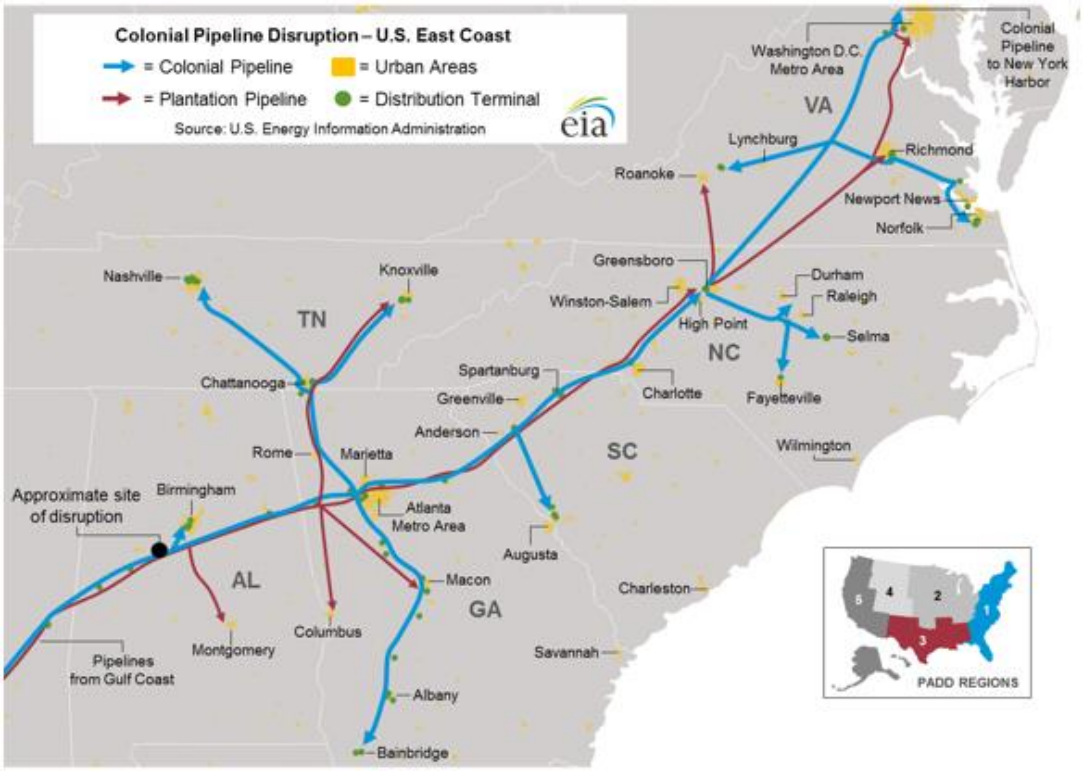

Figure 1: Source - U.S. Energy Information Administration

A cybercrime hacking group, identified as DarkSide, is said to have gained access to their network utilizing a compromised password leaked on the Dark Web that belonged to a user account that was no longer in use but was still able to access the network.

The hackers gained access to Colonial Pipeline's internal network through VPN, used by employees to remotely access the company's network, which didn't require multi-factor authentication.

Once in the network, the hackers stole 100 gigabytes of data within 2 hours and infected Colonial Pipeline's systems with a 75 bitcoin, $4.4 million ransomware attack. This caused the company to shut down its IT systems and pipeline to prevent the ransomware from spreading, which stayed offline for several days, causing a gas shortage on the east coast and triggering President Joe Biden to issue a State of Emergency.

Figure 2: Source - The Guardian

Colonial Systems brought in a Cybersecurity consultant for assistance and paid the $4.4 million ransom to obtain the ransomware decryption key so they could regain access to their IT systems. Luckily for Colonial Systems, the Department of Justice was able to recover approximately $2.3 million worth of bitcoin from the attackers.

Key Outcomes and Findings

After the attack, IT forensic findings identified numerous known and preventable vulnerabilities, such as unpatched and outdated IT systems, that likely led to the cyber breach, in addition to the other glaring vulnerabilities, such as not requiring multi-factor authentication and not disabling unused accounts.

Additionally, Colonial Pipeline now faces multiple lawsuits, including two class-action lawsuits, a lawsuit from the North Carolina Department of Environmental Quality, and others. At a congressional hearing, Colonial Pipeline CEO Joseph Blount testified about the cyber attack.

INSTRUCTOR ALTON

Colonial Pipeline Ransomware

Case Study Analysis

Student Activity: Case Study Analysis Questions

Colonial Pipeline had some obvious shortcomings in managing and protecting its IT infrastructure in the face of this ransomware attack. It appears they had inadequate disaster recovery and business continuity measures in place and were ill-equipped to handle this cyber-attack.

- After reviewing this case study, what are your thoughts and opinions on the Colonial Pipeline Ransomware attack?
- Do you feel that the company lacked proper IT management, IT security management, and risk management?
- How do you think the concepts of due care, due diligence, and gross negligence apply to this scenario?