

Ransomware Attack on Colonial Pipeline Company, May 7th, 2021

Alexander Luna, John Mason, Michael Wehrli
Gabelli School of Business at Lincoln Center, Fordham University

On May 7th, 2021, the cybercriminal group “DarkSide” launched a ransomware attack on Colonial Pipeline Company’s vital operative systems. The encrypted attack vector compromised the company’s billing systems, precipitating a forced and abrupt cessation of operations. In addition to the attack on company systems, DarkSide has stolen 100 gigabytes of private company data, which they have threatened to release unless demands are met. The missing files include private employee information, such as social security numbers, bank routing numbers, military identification numbers, and health insurance records. DarkSide is demanding payment of 75 Bitcoin, approximately \$4,400,000 in value, in exchange for the decryption key and return of stolen data. Colonial Pipeline Company is facing pressure from stakeholders to act swiftly in response to the attack but has been heavily advised by the FBI to avoid any measure of capitulation.

Mr. Luna, Mr. Mason, and Mr. Wherli are representatives of the Fordham Consulting Group, which has been contracted as an ad hoc advisory agent in response to the attack. Our terms are to present Colonial Pipeline’s CEO, Mr. Joseph Blount, with an immediate and effective solution on the afternoon of the attack. Our solution strives to reach resolve while working within the bounds of what is most financially, legally, and ethically responsible. In acting to protect the best interests of the company and its stakeholders, we advise that Mr. Blount pay DarkSide in an attempt to retrieve the decryption key and stolen data. We will begin our proposal by presenting the context; critical facts, actors, and catalysts that will help Mr. Blount make the most informed decision possible. We will proceed to outline our financial and legal analysis, which will guide a lawful and financially viable response to the attack. Once briefed in full, we will make our suggestion to Mr. Blount. This will be supplemented by a thorough consideration of the situation’s ethical dimensions, and our case against alternative solutions Mr. Blount may take.

The pipeline operated by Colonial Pipeline Company is the largest domestic pipeline in the United States and is responsible for delivering nearly half of the east coast oil supply at a rate of 2.5 million barrels per day. With annual revenue of \$1.3 billion, the pipeline generates an average of \$3.56 million in revenue each day. Given the company’s substantial market share, a prolonged shutdown will result in a rapid decrease in profits and significant shocks to the domestic oil market. The resultant decrease in the national oil inventory, coupled with forecasted consumer panic-buying, will dramatically raise the price of gas in the short term. This in turn will harm low-income Americans by greatly reducing discretionary income. Moreover, company shareholders will lose \$1.15 million in income each day the pipeline remains shut down. As a result, we have determined that the most pressing action item is to restore operations, which may best be achieved by meeting DarkSide’s demands. Legally, Colonial Pipelines faces potential employee negligence lawsuits, as well as dereliction of fiduciary duty lawsuits. The FBI guidelines encourage companies to avoid payment, however, Colonial Pipelines is within their legal right to conduct an exchange of ransom payment. Doing so greatly reduces the risk of lawsuits and helps to better protect our valued stakeholders.

We believe that the decision to pay the ransom is the most ethical resolution. In doing so, Colonial Pipelines protects the relative interests of major stakeholders, dutifully honoring the trust they have placed in the company’s management and operations. The proposed solution acts under the fiduciary duty of the CEO, which we believe should be considered an ethical obligation. Furthermore, this decision fulfills standing promises to protect the company’s employees and their private data. Lastly, by seeking to actively avoid detrimental shocks to the economy, we can better preserve the welfare and livelihood of American consumers who depend on our vital infrastructures.

