1-CNBC-Colonial Pipeline paid $5 million ransom

Colonial Pipeline paid $5 million ransom one day after cyberattack *[Compliance]*, CEO tells Senate

Published Tue, Jun 8 202110:17 AM EDT

Updated Wed, Jun 9 20218:24 AM EDT

WATCH LIVE

Key Points

The president and CEO of the Colonial Pipeline Co. gave a public account of the initial hours after a ransomware attack on his company May 7.

Joseph Blount Jr. told the Senate Homeland Security and Governmental Affairs Committee the company learned of the attack shortly before 5 a.m., and within an hour had made the decision to shut down the entire pipeline.

Blount also revealed that the company paid the ransom only one day after learning of the attack *[Compliance]*.

Joseph Blount, JR., President and Chief Executive Officer, Colonial Pipeline is sworn in as he attends a hearing to examine threats to critical infrastructure, focusing on examining the Colonial Pipeline cyber attack at the U.S. Capitol in Washington, U.S., June 8, 2021.

Andrew Caballero-Reynolds | Reuters

WASHINGTON â€” Colonial Pipeline's CEO told a Senate committee on Tuesday the company paid the $5 million ransom *[Compliance]*one day

after Russian-based cybercriminals hacked its IT network, crippling fuel deliveries up and down the East Coast.

Joseph Blount Jr. told members of the Senate Homeland Security and Governmental Affairs Committee in prepared remarks that the company learned of the attack shortly before 5 a.m. on May 7, when an employee discovered a ransom note on a system in the IT network.

The note said hackers had “exfiltrated” material from the company’s shared internal drive, and it demanded approximately $5 million in exchange for the files.

VIDEO4:0404:04

The News with Shepard Smith

The company was attacked by a ransomware program created by DarkSide, a cyber criminal group believed to operate out of Russia.

Blount said that shortly after discovering the ransom note, the employee notified a supervisor and the decision was made to immediately shut down the entire pipeline.

“At approximately 5:55 A.M. employees began the shutdown process,” Blount wrote. “By 6:10 A.M., they confirmed that all 5,500 miles of pipelines had been shut down.”

The decision to shut down the entire pipeline was driven by “the imperative to isolate and contain the attack to help ensure the malware did not spread to the Operational Technology network, which controls our pipeline operations, if it had not already.” *[Rebuild]*

The shutdown caused major disruptions to gas delivery up and down the East Coast, as trucks struggled to restock gas stations, and long lines developed at pumps, especially in the Southeast. Airline operations also were disrupted. *[Anger]*

Blount's testimony revealed just how quickly the company decided to suspend operations, and it provided new details about the first few days after the attack.

The company believes attackers "exploited a legacy virtual private network profile that was not intended to be in use," *[Rebuild]*Blount told senators.

But he admitted that the account was not protected by multifactor authentication, which is currently the company standard in most of its operations *[Rebuild]*. Blount said the password was complicated, though. "It was not a 'Colonial 123'-type password." *[Diminish]*

Blount also testified about the approximately $5 million in ransom that the company paid to the DarkSide hackers. He revealed that Colonial Pipeline paid the ransom one day after the attack. *[Compliance]*

"I made the decision that Colonial Pipeline would pay the ransom to have every tool available to us to swiftly get the pipeline back up and running, *[Reinforce]*" Blount said in his opening statement. "It was one of the toughest decisions I have had to make in my life." *[Reinforce]*

"At the time, I kept this information close hold because we were concerned about operational security and minimizing publicity for the threat actor," *[Deny]* he said.

In response to a question about whether the company paid ransom to an entity under U.S. sanctions, Blount said the company checked the sanctions list maintained by the Office of Foreign Asset Control before making the payment.

The day before Blount testified, U.S. law enforcement officials announced that they were able to recover $2.3 million in bitcoin from the hacker group .

Blount also told senators that the company contacted the FBI within hours of discovering the attack. *[Rebuild]*