5-NPR-Colonial Pipeline

How To Stop Ransomware Attacks? 1 Proposal Would Prohibit Victims From Paying Up

Last week, the Transportation Security Administration announced a new policy which requires pipeline operators to report cyberattacks to the federal government within 12 hours *[Legal Action]* and on Thursday, the White House released a memo to corporate executives and business leaders urging them to take immediate steps to protect against ransomware risks in the wake of attacks on both Colonial Pipeline and the meat company JBS .

“The most important takeaway from the recent spate of ransomware attacks on U.S., Irish, German and other organizations around the world,” said Anne Neuberger, deputy national security adviser, in the memo, “is that companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively.”

Joe Blount, CEO of Colonial Pipeline, says his company did exactly that. He spoke with NPR’s All Things Considered about getting the pipeline safely back online, making the tough call to shut down the gas over a cyberattack *[Reinforce]* and why paying the ransom was “the right decision to make for the country.” *[Compliance]* Listen in the audio player above, and read on for highlights of the interview.

Interview Highlights

On whether operations are fully restored

No, definitely not fully restored. And I think if you talk to anybody who suffered from one of these criminal cyberattacks, they would tell you that it takes months and months and months to restore all your IT infrastructure. In our case, our focus initially was to get the pipeline back up and running safely and as soon as we possibly could. So we got the critical IT structure

put back together. But we have lots and months and months of work ahead of us. *[Reinforce]*

On why the company shut down the gas over a computer system attack

Let me take you back to the early morning of May 7. We knew immediately that there was an issue, and we are programmed to only operate the pipeline if we feel that it's in safe operating condition: it won't cause any harm to employees, the communities we serve or to the environment. So we have what we call "stop work authority" at Colonial; any of our employees has the opportunity to use it. If they identify a risk, their job is to contain it immediately. In this case, a ransomware note came across the screen in our control room. It was immediately recognized, and the control room supervisor immediately decided to shut down the pipeline. It was the right decision to make because you don't know what you have [to deal with] at that point in time. *[Rebuild]*

On his decision to pay a nearly $4.5 million ransom in cryptocurrency

[It was] obviously, probably the hardest decision I've ever made in my career. *[Reinforce]* I've been around this asset for a long time: I've been an employee of Colonial Pipeline for three and a half years, but I've been in the industry for almost 39 now. So once we identified the risk and contained the risk by shutting the pipeline system down and immediately called in cyber experts to help us with identifying further what had been done to our system, one of the things that came up, ultimately, was the ransom and whether to pay the ransom or not.

The conversation went like this: Do you pay the ransom or not? And of course, the initial thought is: You don't want to pay the ransom. You don't want to encourage [hackers], you don't want to pay these contemptible criminals. But our job and our duty is to the American public. So when you know that you have 100 million gallons of gasoline and diesel fuels and jet fuels that are going to go across the Southeastern and Eastern seaboard of the United States, it's a very critical decision to make. And if owning that de-encryption tool gets you there quicker, then it's the decision that had to be made. And I did make that decision that day. It was the right decision to make for the country.

On the government’s role when private companies face cyberattacks and ransom

At the end of the day, it’s a decision that has to be made by the company. … I think that obviously private industry has a responsibility here. Pipelines do invest in cyberware and security. It’s a natural extension of what we’ve done historically, which is focus on the physical security of our asset. So it really pretty much needs to become a private-public partnership.

I think once we complete our investigation into this event, partnering with the government, sharing those learnings with our peers in the infrastructure space and more broadly across other sectors, is very important so that they can learn lessons from our event. *[Rebuild]*

Jason Fuller and Justine Kenin produced and edited the audio of this interview. Cyrena Touros adapted it for the web.

Correction June 3, 2021

An earlier version of this story suggested that Colonial Pipeline waited 6 days to pay the ransom. In fact, it decided to pay the ransom on the same day it got the demand. *[Compliance]*