The recent cybersecurity incident involving the [Colonial Pipeline](https://en.wikipedia.org/wiki/Colonial_Pipeline) offers an incredibly rich vista for exploring a variety of economics concepts. Questions about what went wrong and how to prevent this in the future naturally dovetail with the fundamental questions of economics centering on scarcity, who produces, who consumes, and how much. This post will touch on the public’s non-intuitive (and to many infuriating) behavior in response to the gasoline shortage, questions about market forces and corporate responsibility, and the role of regulation.

But before getting to the analysis a brief recap is in order. The colonial pipeline provides a large percentage ([approximately 45%](https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/)) of gasoline to the eastern United States ranging from the Gulf Coast (eastern Texas and Louisiana), through the south, up along the Carolinas, into the mid-Atlantic states, and into New Jersey and Pennsylvania.

Map

Description automatically generated

On May 7, 2021, the [pipeline was the victim of a ransomware attack](https://en.wikipedia.org/wiki/Colonial_Pipeline_cyberattack), and the company halted all flow to mitigate the attack, which, reportedly, [did not disable pipeline operations but infrastructure support](https://www.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html) (e.g. billing). Even though the company almost immediately paid the requested ransom of 75 bitcoin, equivalent to approximately 5 million dollars, it took about 5 days to totally restore operations and at least a week beyond that for the entire system to return to normal. During the 12 to 14 days of the disruption, the entire customer base suffered, to varying degrees, long gasoline lines and a general shortage of gasoline. Stories about some individuals hoarding the supply surfaced along with widespread speculation about Colonial’s vulnerability to cyberattacks, and as always, the role that government and regulation should play in these situations became a common topic of conversation. This post will content itself with only some of the highlights.

Foremost of these was the public response to the scarcity of gasoline. Once the pipeline shut down, it was only a matter of time before the supply dropped and the price increased. Common wisdom argued that these price increases would trigger a drop in demand resulting in motorists in the effected area minimizing their trips in a car. This interplay between supply, price, and demand is the traditional prediction of classical economics thinking. What happened was a bit more intriguing. If reports are to be believed (as should likely be the case), as the supply went down and the price rose, the demand actually increased to a greater level than had been the case prior to May 7th.

The most probable mechanic behind this paradoxical behavior (at lease according to classical theory) seems to be related to the [prisoner's dilemma](http://commoncents.blogwyrm.com/?p=53). Each member of the gasoline-consuming public could have looked at the situation and said “This disruption won't last long. One way or another gas supplies will increase soon and so I'll cooperate with my neighbor; I will limit my gasoline purchases alleviate the crisis.” However, as in the traditional prisoner’s dilemma, there is a rational fear of being betrayed by other actors in the drama which pressures each participant to betray as well. Each person imagined the possibility of limiting their gas purchase and then came face to face with the fear that the supply of gasoline he really needed would be unavailable if his neighbor, thinking about the situation in the same way, reacted by rushing out to buy more gas than he absolutely required. This self-enforcing negative feedback, which looks to have actually happened, was labeled by the media as ‘panic-buying’ but it seems to be based on something far more rational than blind fear.

The second interesting point to consider is if market forces could have been marshalled that would have led to a better outcome. Obviously, Colonial Pipeline had been vulnerable to this cyberattack but the reason for that vulnerability isn’t forthcoming and, given the sensitive nature, is likely to never be fully known. Nonetheless, this lack of information shouldn’t stop a vigorous analysis of what might have been done differently (although it should stop people jumping to conclusions – but it won’t). The starting point will be the very practical question: did Colonial Pipeline take cybersecurity seriously?

There are practical reasons why any business entity (individual, family, corporation, education institution, etc.) might actually choose to ignore steps to beef up its cybersecurity. As argued by Cormac Herley in his article entitled [*So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users*](https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/SoLongAndNoThanks.pdf), security measures that cost more than the incident they intend to prevent are a non-starter. It is possible that Colonial Pipeline recognized the need for cybersecurity but could only afford so much and they knowingly and calculatedly set aside money for a ransomware attack. After all, ransomware attacks are meant to be annoying not debilitating and paying 5 million dollars occasionally may be more cost-effective than spending 30 million each year on IT. The group allegedly behind this has even stated that they had no intention of causing this much trouble precisely because trouble triggers investigations and they simply want money.

Timeline

Description automatically generated with medium confidence

There are always those amongst us who would argue that a company should ‘do the right thing’ regardless of cost but what, exactly, is the right thing. Would customers be willing to pay 4 cents more per gallon to ensure that this kind of thing would be far less likely in the future? Ask the motorist who was waiting in a 2-hour gas line the answer is likely to be yes but ask that same motorist now that the situation has returned to normal his answer will likely be no.

Perhaps there is a way for Colonial to market their socially responsible position but that notion is farfetched. Most of us know our local gas stations not the company(ies) that they deal with to get gas in the ground for us to pump. Colonial would have to spend millions raising social awareness before they could even begin to recoup that investment and apply it to their efforts in beefing up their cybersecurity.

Finally, there is the overall question of regulation given the optics of this event. The public seems to have acted irrationally and, at lease in some eyes, Colonial Pipeline was also irresponsible for lapses in security and craven in paying the demanded ransom. No doubt some politicians are considering if this situation clearly invites government stepping in and declaring Colonial Pipeline as a public utility. Arguments will surely surface that government needs to do more to ensure that companies keep current in their cybersecurity posture and, given the high-profile nature of this incident and the current ongoing federal involvement, future mandatory compliance seems certain. The regulatory burden that will result will likely be far more expensive than a thorough internal approach. This is the real bottom line incentive for ‘doing the right thing’; that the cure will be worse than the disease.

So, it seems that the Colonial Pipeline incident is literally the gift that keeps giving to professional economist. Scholars and theorists will be busy for decades analyzing every nook and cranny, from new variants on the prisoner’s dilemma, to better market forces designed to incentivize corporate responsibility and the role that government regulation should play in cyberspace. Sadly, for the rest of us, it is a reminder of how the digital world of ones and zeros can have a big impact on the real world of dollars and cents.