The Colonial Pipeline Dilemma

A cyberterrorist group infected Colonial Pipeline's computers with ransomware, which caused the company to shut down its pipeline. The shutdown was so disruptive it made the national news and caused gasoline shortages on the East Coast. The pipeline company paid a $5 million ransom to the terrorists in order to obtain software that would unlock their computer systems.

The Prisoner's Dilemma, the most famous model in game theory, can give insight into why the company paid the ransom, and what the optimal government policy to deal with these terrorist would look like. In a Prisoner's Dilemma, as applied to this case, all companies whose systems have been infected with ransomware act independently. That is, they do not communicate with each other. In this environment, all companies have an incentive to pay a ransom, regardless of whether other companies pay their ransoms. But, companies would be better off if they all agreed to never pay a ransom. If this happened, the cyber terrorists would not bother infecting any company's computer system because they could not gain from doing so. Unfortunately, each company has an incentive to cheat on the "never pay" agreement. Once infected, a company would find it cheaper to pay the ransom than to keep to their agreement.

The way to solve a Prisoner's Dilemma is to get a third-party enforcer, most likely the government, to make sure the companies keep their agreement. The government could ensure compliance to the "never pay" agreement by punishing companies who cheat and by making it difficult for companies to pay the ransom.

First, the federal government could make it illegal to pay ransoms. This would change the incentives company officials face. A company's CEO would often not want to risk being thrown in jail by authorizing a ransom payment. A cyber terrorist group that repeatedly infected company systems with ransomware, but who never got paid, would soon tire of pursuing such a futile activity. As a result, the terrorist groups would stop trying to infect company systems with ransomware.

Even if making ransom payments were illegal, some companies would probably try to make the payments illegally. They might keep their payments secret to avoid prosecution. To deal with this scenario, the federal government should adopt a second policy. The government should seek and destroy the platforms that cyber terrorists use to receive payments. For instance, if a terrorist group receives payments through a website, our government should disable the website to prevent these payments. The government should do everything it can to make it difficult for a company to pay a ransom.

The policies that I have outlined will be troublesome for the next few companies that are infected with ransomware. These companies will want to pay the ransom because it is the lowest cost option that will allow them to resume normal operations. The government policies I mentioned will prevent payments and these companies will likely suffer as a result. However, over time U.S. companies will develop a reputation for refusing to pay ransoms, causing cyber terrorist groups to pick other targets, or better yet, to find other uses of their time.