Demand, supply and cyberterrorists

Cyberterrorists have been busy lately, infecting the computer systems of many companies with ransomware. So far, the victims have included a gas pipeline company, hospitals, and meat processing operations. These companies, once infected, lose access to their computer systems, at least until they pay the ransom or find a way to overcome their computer problems. While their computer systems are down, the targeted companies are usually unable to provide their product to consumers. With less access to these products, consumers are worse off.

Joe McGarrity
Economics Professor

Unfortunately, consumers should expect more of these attacks in the future since the cyberterrorists reside in countries like Russia, which allow the cybercriminals to freely operate. The U.S. government has been unable to convince foreign governments to pursue and prosecute their cybercriminals.

Since these ransomware attacks will probably occur fairly often, it is worth thinking about how the attacks will impact the economy. To help us anticipate the effects of future attacks, we can turn to the demand and supply model. In this model, the price of a product changes to coordinate firms' production plans with consumers' purchasing plans. To help illustrate, consider a market for beef.

Before a ransomware attack, the market for beef would have settled into a situation where firms charged a price that encouraged them to produce about the amount of beef that consumers wished to purchase. Stores did not run out of beef, nor did they see unwanted build ups of their beef inventories. This stable outcome would be disrupted if some beef companies were hit by a ransomware attack that caused them to shut down their operations. On their own, the unaffected firms could not meet the consumers' demand for beef at the going price. Seeking more profit, the firms still producing beef would raise their prices because they could do so and still sell all of their beef. These firms would continue to increase their prices as long as there was a shortage of beef. Eventually, the price would increase enough to discourage consumers from wanting to purchase more beef than firms could provide. The beef shortage would disappear and firms could no longer get away with increasing their prices. Those that tried would be unable to sell their beef. At this point, the market would have reached another stable outcome, where firms are producing the amount of beef that consumers want to purchase; only now, the price of beef is higher than it was before the cyber attack.

Going forward, consumers can expect to see higher prices for goods and services provided by firms that are victims of ransomware attacks. In the face of these risks, people may find it wise to keep inventories of some goods. This way if the company that provides these goods has to shutdown its operations due to a ransomware attack, the people with stockpiles won't get stuck paying very high prices if they need these goods soon after the attack. Similarly, firms that feel that some of their suppliers may be subject to a ransomware attack may want to keep large inventories of their important inputs. These stockpiles will allow firms to avoid paying exorbitant prices for their inputs or even avoid having to temporarily do without them.