CS★T

EDITORIALS COMMENTARY

To protect all of us, government and business had better step up cybersecurity

Last year, nearly 2,400 local governments, health care facilities and schools were victims of ransomware.

By CST Editorial Board | May 15, 2021, 7:17pm CDT

Gas stations in the Southeast ran out of gasoline after Georgia-based gas company Colonial Pipeline reported a ransomware attack on May 7. | Getty

People living in the Southeast can tell you what happens when a critical company, in this case Colonial Pipeline, doesn't shield itself sufficiently from cyberattacks.

Long lines at gas stations. Lives disrupted. Temporarily higher gasoline prices. Companies already trying to recover from the pandemic facing another blow. Four states declaring a state of emergency.

All that happened after Colonial, which carries nearly half the East Coast's fuel supplies, announced on May 7 it had been hit by a ransomware attack.

Editorials

Government and private companies need to step up their security game in a big way. Even a glance at recent events shows how vulnerable we all are because they haven't done enough to guard against cyber intrusions. Despite years of warnings, pipelines, electric grids, power plants and other operations that keep our daily lives running remain ripe targets for audacious attacks.

"There has been a bipartisan lack of attention until now," Matt Erickson, an executive at the cybersecurity firm SpiderOak, told us.

In Chicago, thousands of stolen government emails were published online on April 19, after city officials said they refused to pay a ransom. In Illinois, the attorney general's office announced on May 6 that it is struggling with a ransomware assault in which bad actors froze up computer systems with encryption and demanded payments to restore access.

Last year, a cyberattack linked to Russia on the company SolarWinds admitted foreign actors into computer networks of the federal government and major companies. Last month, a private security firm said Chinese hackers had penetrated federal networks, too.

On Friday, Ireland's health service shut down its IT systems in response to ransomware. In America, bad actors have been snarling hospital systems for years, endangering patients' health.

Last year, nearly 2,400 local governments, health care facilities and schools were victims of ransomware, according to CNN. The Institute for Security and Technology reports the average payment to free up computer networks was $312,493 and that victims last year paid a combined $350 million, three times the amount of the year before.

U.S. Energy Secretary Jennifer Granholm said last week that the attacks show how vulnerable the nation is, including its energy infrastructure.

Protection isn't easy

It's not easy to protect computer networks. A company or agency has to protect itself 100% of the time. Hackers have to get lucky just once. Unregulated cryptocurrencies such as Bitcoin make it easy for criminals to collect untraceable ransoms. The climax of many movies is when the criminals try to collect ransom money and police have a chance to catch them. Cryptocurrencies pretty much eliminate that because they are virtually untraceable.

Part of the difficulty in improving security is that there are so many targets. More than 80% of the energy infrastructure is owned by the private sector. Those companies are sometimes up against sophisticated criminal groups that may be supported by nation-state actors.

"A lot of ransomware enterprises operate as normal businesses with offices full of engineers and tech support staff," Erickson said. "Their customers are people looking to launch ransomware attacks."

In a promising sign, President Joe Biden has signed an executive order to help guard against cyberattacks. He wants companies to adapt new software standards from companies that sell to the federal government and an "energy star" label that tells consumers the software has strong protections.

Biden also wants to create a National Transportation Safety Board-style agency that will follow up after major attacks to document what went wrong. Companies tend to be secretive about security breaches, so other companies can't learn from their mistakes. An NTSB-style agency would be critical in teaching everyone how to plug loopholes.

Congress should act

But Biden's executive order doesn't go far enough. Congress should act to require private companies to meet the same standards Biden is setting for the federal government. Many oil and gas pipelines use cybersecurity standards that are decades old.

The federal government's policy is to not pay hackers because that creates an incentive for them to launch new assaults. But some companies fear they might go out of business if they don't pay, and stolen data will be sold on the dark web.

Everyone can play a role in defending against successful cyber attacks. Ninety-five percent are the result of phishing scams, in which an unwitting person opens an email attachment that appears valid but gives hackers the key to a computer system. Unfortunately, scammers are getting increasingly artful in making their emails appear legitimate.

Although the February electric grid meltdown in Texas wasn't caused by a cyberattack, it illustrated how massive numbers of people can suffer when an important and unprepared service shuts down out of nowhere. Millions of people in Texas were caught without water, heat and food for days in the middle of winter storms.

We can face more of the same. Or we can throw up better defenses now.

Send letters to letters@suntimes.com.