INSURANCE JOURNAL

States Weigh Bans on Ransomware Payoffs

By Jenni Bergal, Stateline | July 27, 2021

As ransomware attacks continue to wreak havoc on police departments, school districts and city and county governments, some state legislators say they've had enough.

At least three states—New York, North Carolina and Pennsylvania—are considering legislation that would ban state and local government agencies from paying ransom if they're attacked by cybercriminals. A similar bill in Texas died in committee earlier this year.

Prohibiting ransom payments would help deter attacks because cybercriminals would know they couldn't get paid and would have no financial incentive, the legislators say.

"If criminals know that Pennsylvania will not pay ransom, we are going to make ourselves a less likely target for these types of attacks," said Republican state Sen. Kristin Phillips-Hill, who is sponsoring a no-ransom bill. "Our citizens' personal information is on the line. We have to do everything we can to protect them."

But some cybersecurity experts say that while banning ransom payments may be well-intentioned, it's a bad idea because local governments, particularly smaller ones, may not be able to restore or rebuild their computer networks quickly. That could prove even more costly and disruptive than paying a ransom.

"Extortion is always wrong. It's bad. But this way, you're punishing the victim," said Dan Lohrmann, chief security officer for Security Mentor, a national cybersecurity training firm that works with states. "I think it could end up causing more harm than good."

Ransomware typically spreads through phishing, in which hackers email malicious links or attachments and people unwittingly click on them. Malware then hijacks the victim's computer system and holds it hostage until the victim either pays a ransom, usually with the cryptocurrency bitcoin, or restores the system on their own.

In recent months, the fallout from ransomware attacks has received widespread public attention. In May, the Colonial Pipeline shutdown sparked panic buying and gas shortages along the East Coast. The company paid more than $4 million to recover its stolen data. In June, JBS, the world's largest meat processing company, paid an $11 million ransom after it was forced to halt operations at its U.S. plants.

Last week, the Biden administration announced the creation of a multiagency task force to combat ransomware and launched a new website to help companies and government agencies better protect themselves.

Hackers frequently take aim at state and local governments. In 2020, at least 113 state and local governments were affected, according to Brett Callow, a threat analyst for cybersecurity company Emsisoft. Nearly 1,700 schools, colleges and universities also were struck.

Hackers have shut down courts, disrupted 911 systems and prevented police officers from checking suspects' criminal histories during traffic stops. They have taken down government websites and prevented residents from paying utility bills or renewing city licenses.

For years, hackers typically didn't steal the ransomed data or make it public. But now, many are downloading files and threatening to release sensitive information as additional leverage if they don't get paid.

Some have made good on that threat.

In May, for example, the city of Tulsa, Oklahoma, was hit in a ransomware attack in which cybercriminals later posted more than 18,000 files, mostly police citations and internal department files, on the dark web. Hackers got access to more than two dozen people's Social Security numbers. City officials, who refused to pay ransom, had to shut down part of Tulsa's computer network and said it could be months before it is fully restored.

The FBI "does not support" paying a ransom in response to an attack. Nor does the federal Cybersecurity and Infrastructure Security Agency, which strongly discourages it.

"Paying ransoms only encourages this malicious activity," Eric Goldstein, the agency's executive assistant director for cybersecurity, said in an emailed statement to Stateline. "Further, paying a ransom provides no assurance that the victim's data will be restored."

State Bans

The North Carolina House was the first state legislative chamber to pass a no-ransom bill. The House approved the measure 114-0 in May, and it is now in a Senate committee.

The bill would bar any state agency or local government entity from paying ransom in a cyberattack.

"The main objective is to take a target off of North Carolina's back," said Republican state Rep. Jake Johnson, one of the bill's primary sponsors. "We're saying we cannot negotiate with you. It's not legal for us to pay anything. You need to stay away from North Carolina."

Johnson, who chairs the House Information Technology Appropriations Committee, also is proposing lawmakers allocate an additional $15 million to help state and local agencies beef up their cybersecurity.

"If you think of a small county, they don't have the capital to go out and hire big firms to do their cybersecurity," he said. "My vision is we would have grants set up that would help counties and local governments that need it."

In Pennsylvania, legislators are considering a broader ransomware bill that would make possessing, using or transferring ransomware a criminal offense, ranging from a first-degree misdemeanor to a first-degree felony, depending on the ransom amount. While these actions could fall under a more general computer crime state statute, the bill would make it a specific offense and increase the maximum penalty.

The measure also would prohibit state and local taxpayer dollars or other public money from being used to pay ransom in a cyberattack. The exception would be if the governor authorizes an agency to do so in the event of a disaster emergency declaration.

“My father-in-law was a firefighter. If you’re trying to put out a fire, the last thing you want to do is pour gasoline on it,” said Phillips-Hill, who chairs the Pennsylvania Senate Communications and Technology Committee. “If they get ransom once, they’re going to come back and try it again. We want to put out the fire.”

Phillips-Hill said it’s not appropriate to use taxpayer dollars to pay ransom to “terrorist organizations, organized crime and nefarious actors working on behalf of rogue nation states.” Many ransomware attacks come from Russia and Eastern Europe, and some have been based in China, Iran and North Korea.

The Senate Judiciary Committee approved the measure 13-1 in June. It awaits a vote on the Senate floor.

In New York, lawmakers have filed two no-ransom bills this session. One bill would set up a grant program to provide $5 million to local governments to upgrade their cybersecurity. It also would bar state and local taxpayer money from being used to pay ransom, starting in 2024, by which time local governments should be able to upgrade their systems.

Another more sweeping measure would ban ransom payments by businesses and health care entities as well as government agencies. It also would require agencies to report ransomware attacks to the state.

Democratic state Sen. Diane Savino, the bill’s primary sponsor, said she figured it would prompt lawmakers to seriously address the ransomware problem. “We decided to introduce the bill like a blunt instrument to force this discussion. Granted, I understand this is probably not the way to go about it. How do we tell private businesses what to do?” Savino said. “But we need to do something. If we continue to just stand back and do nothing, that’s not a solution.”

Savino, who chairs the Senate Internet and Technology Committee, said she plans to hold hearings on the bill this fall before the legislative session reconvenes in January. That discussion will include how the state needs to help local governments pinpoint the vulnerabilities in their systems so they won’t be attacked, she said.

Local governments badly need that aid from states to fortify their systems and to restore their networks if they get hit, said Alan Shark, executive director of the Public Technology Institute, a Washington, D.C.-based nonprofit that provides consulting services to local government information technology executives.

“Without help from the state, it’s like there’s three leaks going on but you only plug up one,” Shark said. “You’ve got to put money into this.”

Thousands of local governments don’t have the expertise or money to pay for robust cybersecurity protection, Shark added. That leaves them especially vulnerable to ransomware attacks.

“There are too many governments out there that have been operating the same way they have for the last 10 years,” he said. “The threat level has ramped up and they haven’t changed.”

A 2019 study by researchers at the University of Maryland, Baltimore County found that local governments are under constant or near-constant cyberattack, “yet, on average, they practice cybersecurity poorly.”

“Serious barriers … include a lack of cybersecurity preparedness within these governments and a lack of adequate funding for it,” the report found.

Making it illegal for local governments to pay ransom to cybercriminals makes sense, and in theory, would make them less of a target, Shark said.

“In the short term, this could cause a lot of pain,” Shark said. “But local governments are going to pay one way or the other: either up front for adequately protecting their systems and data or on the back end, having to pay criminals, which encourages bad behavior.”

Experts Skeptical

Some cybersecurity professionals are skeptical about states banning ransom payments.

“For many local governments it would cost them a lot more money to start over from scratch and rebuild everything, not to mention all the data they would be losing,” Security Mentor’s Lohrmann said.

And even if they were able to rebuild their systems, Lohrmann said, that doesn’t guarantee cybercriminals wouldn’t attack and sell the data on the dark web.

David Kennedy, CEO of TrustedSec, a cybersecurity company headquartered near Cleveland, said a state no-ransom ban could wind up being “catastrophic” for residents.

“It has the ability to shut down entire governments,” Kennedy said. “That means not being able to conduct business. And we’re also talking about possible outages of energy and water treatment facilities that could take months to recover.”

A state law wouldn’t have much impact on ransomware groups anyway because they often use a shotgun approach and don’t necessarily know which organization they’re going after, Kennedy added.

Even if they do figure out which states prohibit ransom payments and which don’t, they might attack anyway, he said.

“If they notice revenue streams going down, they may be thinking, ‘Let’s cause as much pain as possible in these local and state organizations so other states will think twice about cutting ransom payments,'” he said. “I don’t think they’ll stop.”

Emsisoft's Callow agrees that ransomware attacks often are opportunistic and random, so one state passing a ban wouldn't make much difference.

"Ransomware gangs aren't going to hunt around to find out what the various laws are in various states," he said. "This would need to be an all or nothing deal with every state adopting the same legislation. That could have some effect."

Some cybersecurity specialists say lawmakers should pump more money into helping state and local governments strengthen their systems rather than banning ransom payments. That means making sure data is backed up, improving staff training and conducting risk assessments.

"If you really want to stop ransomware," Lohrmann said, "you've got to be proactive."

Source: Stateline, an initiative of The Pew Charitable Trusts.

Top Photo: Drivers fill their tanks in East Ridge, Tennessee, after a ransomware attack on the Colonial Pipeline sparked lines at gas stations and empty pumps in May. Some state legislators are trying to prohibit government agencies victimized in cyberattacks from paying ransom.Matt Hamilton Chattanooga Time Free Press via The Associa

ted Press.

Topics

About Jenni Bergal, Stateline

Jenni Bergal is a veteran journalist who covers transportation, infrastructure, and cybersecurity for Stateline. She has been a reporter at Kaiser Health News, the Center for Public Integrity and the South Florida Sun-Sentinel, and was supervising senior editor of "Weekend Edition" at NPR. Bergal has spent much of her career doing investigative reporting. She has won numerous national awards, including the Gerald Loeb Award for Distinguished Business and Financial Journalism, the National Press Club Consumer Journalism Award and the Worth Bingham Prize for Investigative Reporting and is a two-time Pulitzer Prize finalist. She is a co-author of the book, City Adrift: New Orleans Before and After Katrina. More from Jenni Bergal, Stateline

Was this article valuable?