LAW360® Pulse

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What New Ransomware Pay Bans Could Mean For Law Firms

By **Steven Lerner**

Law360 (July 13, 2021, 10:36 AM EDT) -- As ransomware attacks against the legal industry escalate and some law firms contemplate paying the ransom to eradicate the problem, at least four states are considering legislation that would limit or ban ransomware payments.

A proposal in New York would prohibit businesses, health care providers and government entities from paying a cyber ransom. Another proposal in the Pennsylvania Legislature would ban the use of taxpayer funds for ransom payments. Meanwhile, lawmakers in North Carolina and Texas are proposing bills to stop ransom payments from local governments.

Some of these proposals were created in response to recent high-profile ransomware attacks, including the breach against Colonial Pipeline Co. where the company **paid** the attackers a $4.4 million ransom.

Ross B. Siroti, the CEO of legal IT services and private cloud provider Rekall Technologies, told Law360 Pulse that some law firms pay the ransom when they realize they didn't back up data.

"If you have a good backup, you should never pay a ransom," Siroti said.

Siroti added that none of his clients, which tend to be smaller or mid-size law firms, have ever paid the ransom when they were attacked. He recalled an incident where a 75-user firm on the company's cloud was attacked, but it was contained to just one person in the firm who was unable to open files.

Claudia Rast, Butzel Long PC's cybersecurity group leader and co-chair of the American Bar Association's cybersecurity legal task force, told Law360 Pulse that payments should not be made because they fill the coffers of the attackers.

"But I've been in the room with companies large and small when they learn that their backups are also encrypted and they face business failure, including laying off tens, hundreds, or thousands of employees and disrupting the supply chains of their customers if they don't act quickly to pay the ransom and restore their operations," Rast said. "It's a chaotic and horrible situation that these companies face."

A Post-Ransom World For Law Firms

While there have been BigLaw firms that **have been hit** by ransomware attacks in the last year, including Seyfarth Shaw LLP, smaller firms have also been victimized by these incidents. BigLaw firms are more likely to have the funds to pay the ransom to guarantee that they can recover any data.

Experts agree that law firms might circumvent the patchwork of states prohibiting payment of ransoms if they operate in multiple states without the restrictions.

And while some attorneys may not be fazed by the new state laws on ransomware, experts say that there are some solutions that law firms should implement in order to provide more protection.

"You can't stop ransomware 1,000%," Siroti said. "The best thing you can do is make sure you're in a scenario where you can get back up and run fast and not pay the ransom."

Siroti says it's worth paying more money for a high-quality disaster recovery solution in order to ensure timely restoration of data. He recalls a small firm in Philadelphia that used a cheap backup solution, which resulted in the firm waiting nearly a week before getting back up and running.

And with a business model based on high hourly wages to attorneys, Siroti said that this type of investment can save the firm money in the long run.

"I think it is incumbent upon us as lawyers, from BigLaw to solo practitioners, whose ethical duty includes protecting client information (among many other professional obligations), to examine the steps we can take to minimize ransomware attacks," Rast said. "Even insurance won't help if a firm is prohibited from paying a ransom to recover its encrypted data."

Rast suggested that firms take several steps now to limit the impact of a ransomware attack, including deploying multifactor authentication, endpoint detection and sophisticated response systems that automatically detect intrusions.

She added that law firms should control user access levels to IT systems, mandate virtual private networks for remote access, segment and encrypt data on the IT network and properly train users so that they understand threat actors.

While none of these solutions are foolproof, they provide a better defense against potential ransomware attacks instead of paying the ransom.

"Someone's going to get hit first before other people are protected, and it may be you," Siroti said.

--Additional reporting by Ben Kochman and Xiumei Dong. Editing by Alyssa Miller.
