The Computer & Internet Lawyer

Volume 40 ▲ Number 8 ▲ September 2023

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

The Increasing Risks and Prohibitions Associated With Paying a Ransom After a Ransomware Attack

By Alexander D. Boyd, Kayleigh S. Shuler and Jessica L. Peel

Although all data security incidents have the potential to cause reputational, operational and financial harm to an organization, ransomware attacks are among the most devastating cyber threats facing organizations. Ransomware victims discover that their critical files are encrypted and inaccessible. They often also receive threats that their data has been stolen. Depending on the organization's level of preparation before an attack, recovery options may be limited. Ideally, the organization will have recent, unencrypted backups that can quickly be used to recover data and restore operations. In many circumstances, however, the available backups are also encrypted, are outdated or will take meaningful time to access and utilize. While no organization wants to pay a ransom to a threat actor, in some circumstances that may be the only viable option to avoid the permanent loss of critical data or significant operational disruptions.

Recently, however, states have begun to consider and enact laws prohibiting certain ransom payments. This trend makes it even more important for organizations to invest in their cybersecurity safeguards and preparations.

The authors, attorneys with Polsinelli, may be contacted at aboyd@polsinelli.com, kshuler@polsinelli.com and jpeel@polsinelli.com, respectively.

RANSOMWARE BACKGROUND

Ransomware is a type of malicious software, or malware, where the attacker locks and encrypts the victim's computer files, systems or networks until a ransom is paid. Attackers also increasingly exfiltrate data prior to encryption, thereby allowing the attacker to extort the victim in two ways: (1) by withholding the key to unlock the encrypted data, and (2) by threatening to leak sensitive data on the dark web. In 2021, the FBI received 3,729 complaints of ransomware, representing only a portion of the overall ransomware threat landscape.[1]

EXISTING RISKS FOR MAKING OR FACILITATING A RANSOMWARE PAYMENT

The FBI, not surprisingly, does not advise organizations to pay criminals their ransom demands because the payment contributes to a criminal enterprise, does not guarantee that an organization will regain access to its data and may incentivize more attacks. Moreover, there is typically minimal legal benefit to paying a ransom because payment does not eliminate an organization's

potential notification obligations under applicable data breach notification laws.

Notwithstanding these practical considerations, however, paying a ransom has historically been permitted by law unless the recipient of the funds is on the U.S. Department of Treasury Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List (often referred to as the OFAC List). In those cases, there are potential civil and criminal penalties for making or facilitating ransomware payments. Assessing whether a particular criminal is on the OFAC List is therefore standard practice for cyber professionals involved with facilitating cyber ransom payments. Until recently, however, there were few other legal considerations to the question of whether payment of a ransom is legally permissible.

New State Prohibitions on Paying Ransom Demands

On April 5, 2022, North Carolina became the first state to prohibit state agencies and local government entities from paying a ransom demand in connection with a ransomware attack. The North Carolina law also goes a step further and prohibits government entities from even communicating with ransomware groups.[2] Government entities experiencing a ransom request in connection with a cybersecurity incident are also required to notify the North Carolina Department of Information Technology.[3] The applicability of the North Carolina law is broad and includes any "agency, department, institution, board, commission, committee, division, bureau, officer, official or other entity of the executive, judicial or legislative branches of State government" as well as "The University of North Carolina and any other entity for which the State has oversight responsibility."[4] The law's prohibition on communicating with threat actors is notable, as even victims with no desire or need to pay a ransom will often communicate with threat actors to gain information that can aid the forensic investigation (e.g., information about what data was stolen and from what systems) and to buy time to investigate and inform involved individuals before data is leaked.

Similar to North Carolina, Florida amended its State Cybersecurity Act to prohibit state agencies, counties and municipalities experiencing a ransomware attack from paying or otherwise complying with a ransom demand.[5] The amendments went into effect on July 1, 2022.

The Florida law also requires state agencies and local governments to report ransomware attacks to the Florida Department of Law Enforcement's Computer Crime Center, the state's Cybersecurity Operations Center and the local sheriff within 12 hours of a ransomware incident.[6] In contrast to the North Carolina law, the Florida law arguably does not prohibit communications with the ransomware groups and it does not apply to university boards of trustees or state universities.[7]

The rationale behind the North Carolina and Florida laws is twofold.

First, some argue that a lack of financial incentive (in the form of ransom payments) will deter ransomware groups from attacking government entities.

Second, some argue that constraints on the ability to purchase decryption keys will force government entities to take a more proactive and aggressive approach to cybersecurity designed to prevent successful attacks in the first place.

Regardless of the merits of these arguments, in practical terms, an organization subject to these constraints that nevertheless experiences an attack may face permanent loss of sensitive or otherwise important data and critical services that could become unavailable if a secure backup of the impacted systems is not available or if the systems cannot be restored in a timely manner.

Additionally, North Carolina's prohibition on even communicating with ransomware groups may hinder government entities from obtaining potentially valuable intelligence regarding the scope and nature of the attack through negotiations.

Following in North Carolina and Florida's footsteps, Arizona, Pennsylvania, New York and Texas have introduced similar legislation banning payments by government entities in connection with ransomware attacks.

Pennsylvania's Senate approved a bill banning state agencies from using taxpayer funds to pay ransomware demands, except in cases where the governor declares a state of emergency and authorizes payment.

New York is also pursuing legislation that would broadly ban ransomware payments by government entities, as well as by businesses and health care entities.

Finally, Texas has introduced legislation that would prohibit government entities or political subdivisions from paying ransom demands. To date, the ransomware payment bans in these states have not yet been enacted.

CONCLUSION

While the current state prohibitions on ransom payments may impact a relatively small number of organizations, if legislators continue to take aggressive positions on ransom payments, a growing number of organizations may face additional legal hurdles when recovering from a ransomware attack. Organizations should strongly consider investing in their cybersecurity programs and data backup solutions and practicing their incident response plans.

Notes

1. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
2. See N.C. Gen. Stat. Ann. § 143-800(a).
3. See N.C. Gen. Stat. Ann. § 143-800(b).
4. See N.C. Gen. Stat. Ann. § 143-800(c).
5. See Fla. Stat. Ann. § 282.3186.
6. See Fla. Stat. Ann. § 282.318(3)(c).
7. See Fla. Stat. Ann. § 282.3186.