Not in My Backyard: NC Becomes First State to Prohibit Public Entities from Paying Ransoms

Article By

Patricia A. Markus
Nelson Mullins
Idea Exchange - Alerts

Related Practices & Jurisdictions

- Communications, Media & Internet
- Corporate & Business Organizations
- Administrative & Regulatory
- North Carolina

Tuesday, April 5, 2022

As part of the budget appropriations law enacted on November 18, 2021,[1] North Carolina became the first state in the nation to prohibit state agencies and local government entities from paying a ransom following a ransomware attack.[2] The new law also prohibits public entities from communicating with a malicious actor following a ransomware attack. Instead, such entities must consult with the North Carolina Department of Information Technology (the “Department”) when they experience such an attack.[3] Passage of this law follows a sharp increase in ransomware attacks against state and local governments since 2019.

The new law applies to all local government entities, including cities, counties, local school administrative units, and community colleges. All state agencies—
including boards, commissions, bureaus, officials, and other entities of the executive, legislative, and judicial branches, as well as The University of North Carolina—also are subject to the payment and communication prohibitions.\[4\]

Local government entities are required to report cybersecurity incidents to the Department, while private sector entities are encouraged, but not required, to make such reports.\[5\] Information shared with the Department—including security features of a public entity’s electronic data processing systems, information technology systems, telecommunications networks, or electronic security systems, including hardware or software security, passwords, or security standards, procedures, processes, configurations, software, and codes—is not subject to public disclosure as a public record.\[6\]

A similar bill approved by the Pennsylvania Senate in January 2022 would ban the use of taxpayer funds to pay ransoms following cyberattacks, except where the governor has made a declaration of a disaster emergency and authorized the payment.\[7\] New York also is pursing legislation banning ransomware payments by both public agencies and private companies.\[8\]

Lawmakers in North Carolina and Pennsylvania have suggested that if hackers know that a state or local agency is prohibited by law from paying a ransom, the hackers will have no financial incentive to attack such agencies and accordingly will look for victims in other states. However, categorically prohibiting ransom payments may disadvantage public agencies that have not created back-up copies of their information systems, as they will be unable to restore or rebuild their systems. State and local agencies in these states and elsewhere should make efforts to assure that they have reliable back-up systems, appropriate safeguards for their information technology systems, and adequate cyber insurance coverage.

**FOOTNOTES**


Copyright ©2022 Nelson Mullins Riley & Scarborough LLP