WARD AND SMITH, P.A.
ATTORNEYS AT LAW

The Extortion Economy: North Carolina's New Legislation to Counter Ransomware

Written By Whitney Campbell Christensen (wcchristensen@wardandsmith.com) and **Peter N. McClelland, CIPP/US** (pnmcclelland@wardandsmith.com)

November 18, 2021


On Tuesday, November 16, 2021, Governor Cooper announced his intention to sign a new $25.7 billion budget for the state of North Carolina, essentially guaranteeing that the budget's contents will become law.

One aspect of the legislation that may be overshadowed by the budget's headline-grabbing policy changes is a cybersecurity-related provision buried more than 500 pages into the bill that will have a major impact on public entities of all sorts in North Carolina.

Specifically, the budget will enact a provision from an earlier bill to ban all "state [agencies] or local government [entities]" from paying or communicating with malicious cyber-actors in the event of a ransomware attack. These malicious cyber-actors frequently attempt to extort local governments, businesses, nonprofits, and anyone they can for cash (or cryptocurrency) payments after they launch attacks. Ransomware attacks are incredibly serious because they occur when a malicious cyber-actor gains access to an organization's network or device(s), releases software that encrypts all the data it can find in order to render the network or device(s) unusable, and then demands payment from the organization to have their access to the data restored. The City of Baltimore, for example, refused to pay a ransom demand in 2019 and their budgeting office estimates the incident ultimately cost their organization $18.2 million in direct and indirect losses.

However, under the law, as presented in the North Carolina budget, no state agencies or local government entities would be allowed to pay the ransom to restore access to their systems. And it's not just departments, cities, and towns that the law covers. The law defines "state agency" to include all agencies, departments, institutions, boards, commissions, committees, divisions, bureaus, officers, officials, and other entities of the executive, legislative, or judicial branches, as well as including the University of North Carolina System and any other entity over which the state government has oversight responsibility. What is more, "local government entity" would include local political subdivisions of North Carolina, including, but not limited to, cities, counties, local school districts, and community colleges. And these provisions are effective as soon as the budget is signed, which could come as soon as tomorrow.

This means that whether your organization is a department of state government, a city, a school board, a community college, a county courthouse, or any other state or local government body or subdivision in North

Carolina, the option of paying a ransom for your data in the unfortunate event that an attack like this occurs will be taken off the table on the day this budget gets signed.

That makes prevention of these cybersecurity incidents and preparation for how to respond when they do occur even more important for public entities in North Carolina. There are a number of ways that organizations can reduce the risk of a successful attack hobbling their operations without having to invest taxpayer money in costly technologies (that often have substantial ongoing expenses associated with them), but generally, these methods can only be accomplished proactively.

For example, having incident response plans and operational continuity plans are proven ways to reduce the impact of ransomware attacks and data security incidents of all kinds. Engaging in a data mapping exercise will improve an organization's understanding of their cybersecurity posture and allow expert analysis to craft strategies for minimizing harm. Training an organization's employees will empower them to spot suspicious activity before it begins. All of these will be helpful to avoid the next situation, but once an attack has begun without the pieces of training and plans in place, it can be next-to-impossible to avoid the costliest solutions to address the problem.

At Ward and Smith, we are dedicated to helping clients protect themselves and their stakeholders through expert counsel on data protection. If your organization needs counsel on how to navigate the changing regulatory environment, please contact Ward and Smith's Certified Privacy Professionals, Peter McClelland and Angela Doughty.

--