Bond Case Briefs

Municipal Finance Law Since 1971

Cybercriminals Are Beginning to Master the Exploitation of Public Entities: Squire Patton Boggs

In March, 2020, a smaller municipality of approximately 145,000 people fell victim to a sophisticated ransomware attack. When city officials issued statements to the public that personal information ***was not compromised***, the cybercriminals retaliated. The bad actors flooded the internet and dark web with personal information from a portion of the stolen 200 gigabytes of data, and demanded nearly $700,000 in a ransom payment from the city coffers to make them stop. As a result, not only did the criminals shut down critical city functions with a traditional ransomware attack, they displayed a new and emerging tactic – exfiltration of personal data to extort ransom payments from smaller municipalities.[1] Historically, municipalities have been reticent to pay ransoms, choosing instead to rebuild their infrastructure. However, given that this response is becoming untenable, municipalities are now more lucrative targets.

In particular, smaller cities and publicly funded entities are becoming welcomed targets because they are often underfunded and underprepared for a sophisticated attack. Further, cybercriminals understand and exploit public officials' responsibility to keep the public informed – which often triggers public officials to rush to make public statements prior to understanding the full scope of the attack. In this case, the bad actors leveraged public misstatements to embarrass and strong arm the municipality into paying a pricy ransom (whether city will pay is unclear). But as ransomware attacks become more sophisticated and directed at smaller municipalities at a greater pace, there are certain steps public sector leaders should consider in evaluating their cybersecurity posture and planning for what some say is the inevitable cyber-attack.

The first step in evaluating a municipality's existing cybersecurity posture is to conduct a Cybersecurity Threat Risk Assessment ("Assessment"). The purpose of this Assessment is to identify cybersecurity vulnerabilities in its policies, procedures, and IT environment and to provide remediation strategies as appropriate. As a best practice, an outside team, comprised of an IT firm and cyber counsel, provides a specialized and objective evaluation. Certainly the pandemic is creating distressed situations, which makes the competition for investment dollars stiff. However, a detailed evaluation of the municipality's cyber-risk profile and documented steps taken to remediate any gaps is an easy way to signal to potential investors and ratings agencies that the municipality is worth the investment.

Next, such an Assessment must include a review (or creation) of the municipality's Incident Response Plan ("IRP") – the municipality's systematic and documented method of approaching and managing its response to a cyberattack. At the heart of an IRP is the inherent strategy to first understand the scope of the cyber incident before issuing statements, especially to the public. When smaller cities appear to be disorganized or underprepared in their response, it can alert the public and savvy municipal investors that the city lacked the proper internal controls to protect its sensitive information. This tarnishes the city's reputation and highlights a poor cyber-risk mitigation strategy, which hurts public confidence and possibly the receipt of much needed investor capital.

Finally, municipalities should test their IRP via a mock cyberattack exercise to make sure that key

people know what to do, who to contact, how to communicate to the public, and how to respond to the crisis, especially in the current operating environment where many officials likely will have to control the situation with a remote response force. Remember, many IRPs were developed prior to the pandemic and may not be easily executed in today's operating environment.

With a little up front planning, smaller municipalities can show potential investors that they have mitigated their cyber-risk in the wake of this new cyber tactic. After all, and no matter the goal, the front-end cost of an Assessment and IRP will be far greater than potential recovery efforts absent one – as exemplified by the $700,000 ransom recently demanded.

Our Data Privacy & Cybersecurity, Restructuring & Insolvency, and Public Finance Practices are well-positioned to help navigate what risks impact the public sector. We can also assist in overall cybersecurity compliance efforts and help develop integrated compliance policies that can be administered effectively and efficiently in the face of uncertain times and operating environments.

[1] See, e.g., *LA County Hit with DoppelPaymer Ransomware Attack*, (last accessed April 26, 2020).