FTR Now

Municipalities are Under Threat of Ransomware Attacks: Are You Prepared?

Date: October 9, 2019

A recent wave of ransomware attacks across North America highlights the emerging risk of cyberattacks on municipalities and municipal agencies and boards. Are you prepared?

What is a Ransomware Attack?

Ransomware is a form of malicious software that infects a network and encrypts systems and files. The encryption is usually accompanied by a message demanding payment in exchange for restoring access to the encrypted data. Payment is generally demanded in bitcoin (a decentralized digital currency).

Most ransomware attacks are launched either through direct hacking into a vulnerable system or through phishing emails that urge municipal employees to click on files or links that then install malware that encrypts systems and files.

Recent Examples

Public institutions across Ontario and North America have been held hostage by ransomware attacks. The *New York Times* reported that over 40 municipalities in the United States have been hit with ransomware attacks already this year, including a simultaneous attack on over 20 municipalities in Texas. Municipalities in Canada are also emerging as targets – with numerous recent attacks on Ontario municipalities, only some of which have been covered in the news.

Are You Ready in the Event of an Attack?

Municipal data security programs must treat the ransomware risk as a priority. Elements of a defendable data security program include enforcing least privilege access to data, two-factor authentication, access controls, and an ongoing information security awareness program that promotes strong phishing awareness. Of particular importance to the ransomware threat is a robust offline data/system backup capability.

We recommend that municipalities review their preparedness for responding to a cybersecurity incident such as a ransomware attack. A prepared municipality has:

- an incident response protocol that provides for timely and decisive decision-making;
- assessed its cybersecurity insurance needs and purchased appropriate levels of insurance coverage; and
- pre-retained an incident response coach (and possibly other service providers) who can provide immediate assistance in the event of an incident.

Put Hicks Morley's Experience to Work For You

Hicks Morley acts as regular information and privacy counsel to many Ontario municipalities and understands the unique demands that municipalities face. We also have over a decade of experience with data security incident response, are the Ontario School Boards Insurance Exchange preferred incident response law firm and have helped with numerous ransomware incidents in the past two years.

Get in Touch

If you would like to discuss cybersecurity preparedness or need help with a ransomware or other data security incident, please contact Dan Michaluk at 416.864.7253 or Matin Fazelpour at 416.864.7213.