CYBERSECURITY LAW ALERT

March 10, 2023

By: Leora Ardizzone, Esq.
Richard Frankel, Esq.

RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.

Municipal Cybersecurity: Securing Critical Systems

"Your network has been penetrated…"

With alarming frequency, these five words are appearing on municipal work stations throughout the nation. They are the last five words anyone sitting in front of a computer wants to see, since these are usually the opening line of a ransom note from a ransomware attacker. Unfortunately, the ransom note is the last stage of a cyber-breach that may have been going on "behind the screen" for days or months, during which the attacker has probed the weaknesses in your system, utilized passwords by logging the keystrokes of your personnel and has exfiltrated data. The bad guys know that state and local government systems house key data about taxpayers, real property and personnel, and operate critical services including 911 systems, traffic lights, waste management monitoring systems, etc. Holding these systems ransom can yield significant returns on the bad guy's investment in the software and time it takes to infiltrate and shut down a network.

Atlanta, GA, Baltimore, MD, and Suffolk County, NY, are municipalities recently crippled by ransomware. Cybercriminals are particularly drawn to state and local government systems because they are fragmented and lack unifying cybersecurity frameworks, yet engage in ever expanding digital technologies and apps that allow for interconnectivity among government agencies and between the government and the citizen. At the same time, our state and local government agencies are using outdated systems, and often lack funding to invest in the necessary personnel and other resources to protect their networks and our information. Although many cyber breaches in local government offices affect relatively small numbers of people, in too many cases, the data is of a sensitive nature, including personally identifiable information of tax payers and municipal employees putting them at risk of identity theft and other financial crimes. Moreover, attacks on government cyber systems such as 911 systems, traffic light systems, and other critical infrastructure put citizens at immediate risk to their life and safety.

Governments, like private enterprise, can take steps today to mitigate the risk of a cyber-breach by adopting certain low or no cost security protocols. The Federal Bureau of Investigations and the Department of the Cybersecurity Infrastructure Security Agency have circulated numerous alerts and bulletins targeted to a variety of industries, frequently with the same recommendations that municipalities should implement immediately. First among them is to take an inventory of their cyber assets and conduct a risk assessment so that the greatest weaknesses in their systems can be identified. A good risk assessment allows for a prioritized approach to come up with a strategy to improve cybersecurity.

In addition to the risk assessment, municipalities should immediately implement the following cheap and easy fixes to add layers of security to their systems:

- Password Management: Municipalities should require employees to change their passwords every 60-90 days, and select passwords that are of sufficient complexity so as to not be easily capable of being guessed by threat actors. Strict no sharing policies should be implemented and enforced as well as imposing timeout sessions at employee work stations so that unattended work stations are locked and the employee is required to log in again.

- Multifactor authentication: In addition to having unique passwords that are changed regularly, municipal employees should also be prompted to input a temporary code that is sent to by email or text message to the employee to gain access to municipal systems. Many applications and programs already in use by many municipalities offer this feature and implementing it would be a cost effective tool in the war against cybercrime.

- Endpoint Detection Monitoring: Although these are more expensive options, endpoint detection monitoring is fast becoming a requirement in any cybersecurity tool kit. These systems can detect, notify appropriate personnel and even block code/software that does not belong in the network or that is acting in an unusual manner.

- Encryption: Encryption converts data into unreadable scrambled code that can only be read by an authorized person having a password or key that is recognized by the system.Data can be encrypted at rest and in transit, and data should always be encrypted when it is housed in portable devices. Many devices are sold with encryption options but for municipal agencies that issue portable devices like laptops, ipads and USB drives, encryption should be a requirement and not an option.

- Patch and update: Software developers are constantly updating their software to respond to cyber risks. It is vital that municipal agencies, like all users, update their hardware with patches and other software updates to ensure that the latest security tools against the latest cyber threats are on their systems.

- Training: Ongoing training of staff in the importance of cyber-hygiene is a relatively low cost way of heightening awareness of cybersecurity. Training must include more than a one hour video once a year, but should include regular reminders to staff to recognize risks as well as ongoing mock phishing tests throughout the year.

- Back-ups: A good back up system is one of the most important ways to mitigate against the worst of the consequences of a cyber-attack. A system that is encrypted, backed up to offsite storage and is segregated from the network ensures that the municipality will be able to restore its systems after a breach. Equally important to regular back-ups is testing the back-ups to ensure that they are protected. Although more costly, redundant back-ups an ideal way to ensure that data can be restored quickly after a breach.

- Incident Response Plan: Having an effective strategy in place to respond to a breach is one of the single most important tools for a municipality to have in place. Much like planning for a flood or fire, municipalities that have effective cyber incident response plans are best able to reduce the adverse impact of a cyber-attack, return the systems to normal operations and provide the citizens and municipal employees with the peace of mind of knowing that their local government has the situation well in hand.

Upon implementing the items bulleted in this article, every municipality should turn to its cybersecurity policies and procedures. This is a more labor intensive effort but well worth the effort. Developing and adopting robust cybersecurity policies requires the municipality to examine every facet of its cybersecurity framework and determine on the best course for mitigating its risks of getting hacked. The great thing is that no municipality has to reinvent the wheel.HIPAA provides a great framework for any municipality that is serious about cleaning up its cyber awareness and risk profile. Nearly every industry in the country that has adopted privacy and security standards for electronic data has nearly identical standards as those promulgated under HIPAA.Likewise, the NIST Cybersecurity Framework provides relatively easy to follow steps for any organization to evolve its cybersecurity, so that any municipality with any budget can take the first steps towards creating a more secure network for itself, its employees and the citizens. However, for any municipality's cybersecurity framework to be effective, it must be recognized as part of day-to-day operations and budgets, with adequate personnel and money to develop and mature so that it can protect itself and the data it is responsible for, from and against ever evolving threats.

For more information, please contact:

Leora Ardizzone, Esq.
(516) 663-6538
lardizzone@rmfpc.com

Richard Frankel, Esq.
(516) 663-6534
rfrankel@rmfpc.com