Click, Breach, Repeat? Cybersecurity Wake-Up Call for Manitoba Municipalities

Authors: Jennifer S. Hanson Jeffrey Kowall

published 10/15/2025

The recent *Auditor General Report on Municipal Allegations and Gaps in Provincial Oversight* released on August 28, 2025, emphasized that cybersecurity should not just be "on the radar" for municipalities but that cybersecurity policies and protocols should be prepared and implemented by municipalities that have not already done so.

The Auditor General found that a municipality failed to investigate a cybersecurity incident for root cause, missing a critical opportunity to understand how the incident occurred and how to prevent future breaches. The Auditor General confirmed that this incident "highlights the need for all municipalities to implement controls based on a recognized cybersecurity framework, to protect them from cybersecurity threats."

Recommendation 1 from the ***Auditor General Report*** was that all municipalities implement, at minimum, the **Canadian Centre for Cyber Security's baseline cybersecurity controls** where they are not already implemented.

Assessing Your Municipality's Cybersecurity Readiness

Has your municipality implemented any cybersecurity controls?
Do you meet the baseline requirements?
Do you meet your required **legal obligations**?

The hours after discovering a security breach are crucial to ensure a timely cybersecurity incident assessment and response. Beyond being an important factor in restoring functionality to your systems expeditiously, having proper policies and protocols in place will help your municipality ensure its compliance with the legal requirements relating to data protection and cybersecurity breaches in a timely manner and mitigate against potential legal liability.

Having a regularly tested **incident response plan** in place means that in the event of a security breach, required steps are taken and no time is wasted.

Key Questions for Municipal Leaders

To ensure that the recommended baseline controls and your municipality's legal obligations are met, consider the following questions:

- **Policy and Procedures:**
  Does your municipality have the appropriate policies, procedures and processes in place to address its privacy, data protection and cybersecurity risks and compliance obligations?

- **Training and Awareness:**
  Do your employees have the appropriate degree of awareness, knowledge, skill and training to effectively deal with the sensitivity of the data being held and to address the applicable privacy, data protection and cybersecurity risks?

- **Data Management:**
  Does your municipality have a full understanding of the data it stores (including all personal information), where it is stored, who has access to it and how it is being used?
- **Incident Response:**
  Does your municipality have a formal incident response plan to deal with a breach of security safeguards that it regularly tests and updates?

Coordinating Efforts

Coordinating efforts with your senior management, technology team and legal advisors is crucial to ensuring that your municipality is best prepared for a **cybersecurity incident** when it occurs.

Learn more about how TDS can support you with your legal needs. If you need assistance with any legal matters, please complete the Client Intake Form on our website at **www.tdslaw.com/intake-form/**.

While care is taken to ensure the accuracy for the purposes stated, before relying upon these articles, you should seek and be guided by legal advice based on your specific circumstances. We would be pleased to provide you with our assistance on any of the issues raised in these articles.

