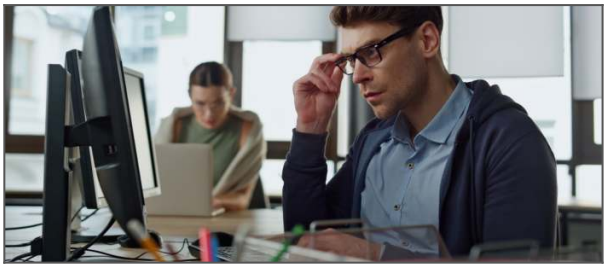
Cybersecurity: Is your Municipality Prepared for a Cyber-Attack?

Authors: Kendall (Dell) Dyck, **Jennifer S. Hanson**, **Jeffrey Kowall**

published 03/22/2024

The question is not *if* a municipality will have a cyber-attack, the question is *when* it will occur.



Victims of a cybersecurity attack are no longer just those which have been traditionally seen as the likely targets, such as large-scale financial institutions or other high-profile gatekeepers of valuable information. Today, all municipalities, regardless of scale, should be prepared for a cybersecurity incident.

Municipalities are subject to *The Freedom of Information and Protection of Privacy Act* (Manitoba) ("FIPPA"), which includes specific obligations with respect to safeguarding the personal information a municipality collects and notification of individuals in the event of a security breach. As of January 1, 2022, failure to comply with FIPPA's breach notification requirements may result in a fine of up to $50,000.00.

Is your municipality ready to respond in an organized and timely manner to a discovery that its information system has been breached, confidential data and personal information has been accessed and its systems are no longer functioning properly? Does it have a formal plan to restore system functionality, identify the information that has been accessed, engage with the applicable regulators, and contact and respond to those whose personal information may have been accessed?

The hours after discovering a security breach are crucial. A timely cybersecurity incident assessment and response is crucial. Beyond being an important factor in restoring functionality to your systems expeditiously, having proper policies and plans 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.

All municipalities should have policies and procedures in place to deal with cybersecurity incidents. This is an area that is constantly evolving, so these policies and procedures should be regularly reviewed and tested to ensure they remain effective and compliant with legal obligations. If your municipality does not have these policies and procedures, or if they have

not been recently reviewed, the questions below will highlight some key considerations to help your municipality ensure that its legal obligations are being met:

- Can your municipality identify its data protection and cyber security compliance obligations?
- Is your municipality aware of the relevant privacy laws that govern it (e.g. FIPPA)?
- Does your municipality apply security safeguards, both technological (such as firewalls, anti-malware and intrusion detection system) and physical (such as locked doors, access cards and security cameras), appropriate to the sensitivity of the data it holds?
- Does your municipality know all the types of data it holds, where it holds the data, how the data is protected, and who has access to the data?
- Does your municipality have the appropriate policies, procedures, and processes in place to address its privacy, data protection and cyber security risks and compliance obligations?
- 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 address the applicable privacy, data protection and cyber security risks?
- Does your municipality evaluate and manage privacy, data protection and cyber security risks arising from its use of third-party contractors or service providers?
- Do your contracts require your service providers to assist you in complying with your regulatory obligations if they suffer a security breach that impacts the personal information for which your municipality is responsible?
- Does your municipality have a formal incident response plan to deal with a breach of security safeguards that it regularly tests and updates?

If you answered “no” to any of the questions above, we suggest that you consult the authors, , or to ensure your municipality has the proper policies, procedures, and response plan in place to effectively deal with a cyber-attack, security breach, and the potential risk of unintended disclosure.

If you answered “yes” to all the questions above, we suggest that your municipality ensure that periodic reviews of your policies and procedures are undertaken.

This article was written for Municipal Leader magazine and is reproduced with permission.

---

this article. The authors are not able to provide free legal advice. If you are seeking advice on specific matters, please contact Keith LaBossiere, CEO & Managing Partner at kdl@tdslaw.com, or 204.934.2587. Please be aware that any unsolicited information sent to the author(s) cannot be considered to be solicitor-client privileged.

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.

