Protecting Your Data in the Digital Age

Brian Rosenbaum — Senior Vice-President, Financial Services Group, Aon Reed Stenhouse

Hardly a day goes by without a news story about a data breach or cyber extortion attempt somewhere in the world, and Canada is certainly not immune. It is also fairly clear that every organization — no matter its size, industry sector, structure, or location — has some degree of cyber exposure. These are the typical cyber risks:

- Disclosure or loss of personal identifiable information of employees, customers, or clients which the organization has under its care, custody, and control
- Failure to protect confidential business information which the organization has under its care, custody, and control
- Network interruption and shutdowns which result in a loss of income for the organization and/or its clients/customers
- Physical damage to property and personal injury to employees and invitees as a result of a breach into infrastructure computer systems

Unfortunately, municipalities generally face all these exposures. They collect a tremendous amount of employee and resident personal identifiable information. They hold confidential and sensitive intellectual property of their business partners. They conduct commerce online, and they are generally responsible for ensuring that buildings and individuals within their municipality are not subject to hacking and/or extortion incidents that can cause damage and personal injury.

DATA BREACHES IN LOCAL GOVERNMENTS

There is a long list of provinces, states, cities, counties, and municipalities that have been the subject of cyber incidents over the past few years. Privacy Rights Clearinghouse, a non-profit website that has tracked data breaches in North America since 2005, lists 723 cyber incidents affecting approximately 179 million data records. These records contained personal identifiable information of employees and/or residents.

Although some of the biggest data breaches have involved cities in the U.S. (such New York, Chicago, Los Angeles, and Indianapolis), Canadian cities are not immune from attacks. According to a 2016 study conducted by a security software company, Malwarebytes, Canadian cities and local governments are very susceptible to malware attacks. The top 10 city targets in Canada this past year were Toronto, Ottawa, Montreal, Markham, Calgary, London, Edmonton, Winnipeg, and St. Catharines.

Of course, not all data breaches are the result of hacking. Municipalities have certainly had their share of employee-error related incidents, such as the Durham Region of Health breach, where a nurse lost an unencrypted thumb drive in a parking lot. The drive contained health information of 81,000 individuals, and its loss resulted in a class action lawsuit.

Budgetary constraints, which are far more significant than those in the private sector, affect municipalities' ability to train staff, and maintain, upgrade, monitor and test their computer systems. To reduce costs, municipalities tend to outsource a high percentage of their IT operations to third parties, including cloud service providers, which can — in some cases — increase risks. Hackers and extortionists target local governments not only for financial gain, which is the prime motivation for cyber-attacks in the private sector, but to make political statements or just plain cause mischief.

All this presents a more significant risk profile for municipalities than other types of organizations. Public scrutiny on the effectiveness of local governments to protect personal identifiable information can be far more intense than in business sectors. Finally, municipalities can be burdened with complex legal compliance obligations if they engage in commercial activities outside their core mandate.

The costs incurred by public-sector organizations to manage, mitigate, and resolve data breaches are staggering.

THE PERCEPTION OF RISK

The tremendous volume of cyber incidents involving municipalities has certainly shaped the opinions of municipal officials and the public. For the second consecutive year, cybersecurity ranked as the top technology priority for U.S. municipalities according to a survey conducted by The Public Technology Institute. A May 2016 Ipsos poll conducted on behalf of Accenture shows 56 per cent of Canadians describe municipalities as vulnerable to a security breach, more vulnerable in fact than federal and provincial governments.

THE UNIQUE CHALLENGES FOR MUNICIPALITIES

Municipalities also face unique challenges in managing cyber risks.

COSTS OF MUNICIPAL DATA BREACHES IN CANADA

If negative public opinion associated with a data breach isn't bad enough, the costs incurred by public-sector organizations to manage, mitigate, and resolve data breaches are staggering. According to a 2015 study conducted by the Ponemon Institute, the cost of a data breach for Canadian public-sector organizations — including municipalities — was $153 per data record. If you take into account the number of records in even a small municipality, it adds up quickly. A multiple-million-dollar loss is not difficult to imagine.

CYBER BEST PRACTICES

Although upgrading IT solutions as part of best practices can be costly and therefore challenging to municipalities, it is only a small part of the governance story. Implementing and policing appropriate policies and procedures have proven to be as effective, if not more effective, in mitigating cyber risks. They do, however, involve an investment of mental and cultural energy, and a great deal of time.

The federal and provincial privacy commissioners regularly publish free guidance on privacy best practices generally, and specifically for municipalities. For example, this past June, the Saskatchewan Information and Privacy Commissioner published privacy breach guidelines with several valuable tips applicable to public bodies. Similar reports aimed at helping public bodies create an appropriate culture of privacy through the implementation of policies and procedures are available online on a regular basis. This report and other privacy information can be found on the Office of the Saskatchewan Information and Privacy Commissioner at *www.opic.sk.ca*.

CYBER RISK TRANSFER AND INSURANCE

Apart from implementing and executing best practices, what options are available to municipalities in managing cyber risk? For starters, a municipality can retain all or part of the exposure and self-insure. Given the significant costs of data breaches, this approach may negatively affect the health and wellbeing of the municipality. In situations where municipalities are using third parties to fulfill all or part of their IT needs, they can attempt to transfer risks through contract — though municipalities should check those service contracts closely to ensure they are protected.

Perhaps the most economical and practical way a municipality can transfer its cyber risk is through the purchase of a cyber and network liability insurance policy. This type of insurance is designed to cover a wide variety of costs and losses in a privacy breach situation. To mitigate its losses and comply with laws and regulations, a municipality will often be required to notify individuals whose personal information has been compromised. The costs to notify, as well as other front-end expenses such as those involving public relations, a call centre, computer forensics, and credit monitoring incurred by a municipality can all be covered under a cyber insurance policy. In the event a lawsuit is brought against a municipality, the insurance will also provide coverage for the legal costs to defend the action as well as any settlements and judgments. There is also potential coverage to terminate an extortion, and in certain situations for business interruption losses as a result of a network shutdown. It is highly recommended that municipalities at least consider the purchase of cyber insurance and engage a knowledgeable insurance professional to assist them.

It is highly recommended that municipalities at least consider the purchase of cyber insurance.