CYBER INSURANCE

Holding taxpayers at ransom

How cybercriminals are stealing municipal data – and how to prevent it

BY JAMES STEELE, *Lawyer, Robertson Stromberg LLP*

Canadian municipalities are among the prime targets for potential cyber attacks. That's why it's vital that they have adequate insurance protection. Only through cyber coverage can Canadian municipalities adequately recover their costs associated with such things as investigation, restoration of data, notification to those compromised, and payment of the actual ransom.

Ransomware is a common type of municipal cyberattack. A network is infected with malware, encrypting data on the systems. This "locked" information can only be retrieved with an encryption key, which is released only after the payment of a ransom. Payment is usually demanded in bitcoin or some other form of cryptocurrency.

Municipalities shouldn't assume that their existing insurance is enough. For instance, general liability policies often do not cover damage to electronic data. Some property policies may limit coverage to loss of use of tangible property resulting from a physical peril.

Fortunately, an increasing number of cyber insurance offerings are available. As with standard insurance policies, packages can vary. Rick Orr, owner of Orr Insurance & Investment in Stratford, Ont., categorizes cyber polices into the following four broad areas of coverage:

Security and privacy liability
Covers liabilities arising from third-party demands or damages due to a privacy breach.

Network or business interruption
Covers the actual loss of revenue for the shutdown period.

Event management coverage
Provides for services required in the event of an attack. Services include the expertise of lawyers, cyber experts, and public relations firms. Also, system forensic teams will help to determine:

- what happened
- how to make the system secure again
- the cost to restore or recreate data
- privacy breach notification costs

Ransomware coverage
This involves a consideration of how to pay for the actual ransom sum, if one is to be paid.

> "If mayors across the country do not start working together on a national strategy, more communities may be hit by online criminals seeking to hold municipal data for ransom."

Are municipalities purchasing cyber insurance? Exact statistics are difficult to obtain. Anecdotally, Orr reports that smaller Canadian municipalities appear less likely than larger ones to carry cyber insurance coverage. This could be for a number of reasons, such as concerns about premium costs or the process required to obtain the coverage.

Some municipal administrations may have yet to plan for the hard reality that they are in fact potential targets; if breached, their own budgets will pay for any uninsured recovery costs. Orr notes that numerous municipal associations such as the Association of Municipalities of Ontario and the Federation of Canadian Municipalities are now taking a more active role in educating their members about cyber risks.

For municipal councils who still believe that an attack on their municipality is too unlikely to warrant cyber insurance, a review of recent attacks in Canada suggests otherwise.

Cyber criminals hijacked Stratford, Ont.'s computer servers last April, locking out municipal employees. The city confirmed the incident was a ransomware attack. Speaking to media at the time, Stratford Mayor Dan Mathieson said Canadian municipalities are "sitting ducks" for cyberattacks. He added that if his fellow mayors across the country do not start working together on a national strategy, more communities may be hit by online criminals seeking to hold municipal data for ransom.

In another example, Mekinac, Que., a regional county municipality, was the victim of a ransomware attack last September, when employees arrived to find their systems locked. Cyber criminals demanded a ransom of eight bitcoins (approximately $65,000) to be deposited into a bank account. The regional county's IT department eventually negotiated the ransom's price down to the equivalent of $30,000. However, the ordeal left the region's servers disabled for two weeks.

Around the same time, Midland, Ont., was also hit. Midland had just purchased cyber insurance months earlier, ironically, because nearby town Wasaga Beach had just been attacked. The Wasaga Beach attack likely brought home the reality to Midland that no one is immune from attacks. A ransom eventually had to be paid by Midland's insurer.

As these attacks demonstrate, brokers need to review carefully what policies will best protect municipalities. Discussions with clients should address factors such as:

- The number and importance of the municipality's online records
- The type of online security protections and protocols already in place
- Training for municipal staff on cyber safety and avoiding phishing scams
- The degree to which a municipality's systems are segregated to avoid a total system-wide breach
- Prior data breach history
- Coverage limits required to respond adequately to a breach

As threats intensify, municipal cyber insurance is necessary to protect taxpayers.

Cyber is a relatively new insurance product and so a broker's advice and assistance can prove critical. For example, when an insured purchases a simple commercial general liability policy, the terms are highly standardized because of the policy interpretations contained in previous court decisions. In contrast, cyber policies are new products, and great variances can exist between policies. As a result, brokers must work closely with their clients to be absolutely sure they understand what they're buying. cu

James Steele is a lawyer with Robertson Stromberg LLP in Saskatoon. He advises and represents clients on insurance coverage matters.

BY THE NUMBERS

FIRST-QUARTER NIGHTMARE

Canadian P&C industry results didn't look pretty in 2019 Q1. In most relevant categories, the year's opening results were worse than during the same time last year (and they weren't good last year). Here's a year-over-year comparison of some choice financial indicators.

($ millions)	2019 Q1	2018 Q1	Thumbs Up (Green)/ Thumbs Down (Red)
Direct Premiums Written (DPW)	$12,888	$11,798	+9.2%
Net Premiums Earned (NPE)	$10,553	$11,249	-6.1%
Operating Expenses	$3,836	$3,671	+4.5%
Underwriting Income	($756)	($119)	-535.3%
Net Investment Income	$1,209	$552	+119%
Net Income	($103)	$196	-152.6%
Combined Ratio	107.7%	101.5%	+6.2%
Net Loss Ratio	71.4%	68.9%	+2.5%
Return on Equity (ROE)	2.4%	4.3%	-1.9%
MCT Ratio	240.7%	240.8%	-0.1%