TOWN OF MINTO

DATE: September 25, 2018
REPORT TO: Mayor and Council
FROM: Gordon Duff, Treasurer/Deputy CAO
SUBJECT: Cybersecurity Insurance

STRATEGIC PLAN:

5.7 Adopt and maintain fair and transparent procurement policies and by-laws to ensure the Town receives competitive pricing on tenders and proposals, and that local business has equal opportunity to submit bids.

BACKGROUND:

Cybersecurity has been of increasing concern in smaller municipalities especially in the past few months. Several municipalities and small to medium-sized businesses have been attacked through viruses in e-mails. This causes data bases to be seized and encrypted with demands for payment before they can be unlocked (ransomware) and fraudulent transfers of funds out of business bank accounts. Many of these organizations had good back-ups of their data, but these back-ups were also lost to ransomware. In 2018, the City of Cambridge, City of Hamilton, Wasaga Beach and Midland have been hacked with losses of data, privacy and cash and there may be more which have not been made public.

While the Town has up to date firewall and anti-virus protection and uses other cyber security controls, our systems are still vulnerable to sophisticated attacks. The Town utilizes both on premises and off-site back-ups with data being saved on an hourly basis. It is often perceived that smartphones and the use of social media have increased the risk of cyberattacks, but a recent study has found that desktops and laptops are far more susceptible to these attacks than smartphones. 59% of infections are transmitted through malicious e-mails or attachments with a further 24% resulting from interactions with suspect web-sites. Our insurance representatives have said that 65% of claims were triggered by human error.

COMMENTS:

Our insurance carrier, JLT, offers additional insurance which covers certain cybersecurity losses. The underwriter for this policy is CFC Underwriting Ltd which is headquartered in London, England and provides service to over 50,000 businesses in over 60 countries. Broadly speaking, this policy covers cyber incident response, cyber-crimes, system damage and business interruption, network security and other related costs. The policy covers the costs for legal and IT consulting to respond to a cyber incident, direct costs associated with the security breach, extortion, restoration of data and other business continuity expense. There are detailed limits and exclusions outlined in the policy.

Staff attended seminars on risk management in the past, however, with this increased threat, more education regarding potential hazards and safe data handling is required. Frequently these training opportunities are offered by insurance companies at little or no cost. The proposed policy includes a cyber risk management portal with webinars, tools and tips which would be available to Council and staff.

FINANCIAL CONSIDERATION:

On an annual basis, the premium for $5 million per claim coverage is $10,250 while that for $2 million per claim coverage is $4,000, all with no deductible for cyber incident response and a $10,000 deductible for internal cybercrimes.

RECOMMENDATION:

That Council receives the report dated September 25, 2018 from the Treasurer/Deputy CAO and provide direction to staff as to which, if any, additional insurance policy should be purchased.

Gordon Duff, Treasurer/Deputy CAO