# FEDERATION OF CANADIAN MUNICIPALITIES

## RESOLUTION SUBMISSION TO SEPTEMBER 2019 BOARD MEETING

BOARD RECOMMENDATIONS
Municipal Finance & Intergovernmental Arrangements

Recommendations for adoption:

1. Adopt the item, as presented.

Recommendations for referral to staff:

2. Direct staff to develop, for the March 2020 Board meeting, an action plan to advance FCM's policy on cybersecurity and ransomware, including reference to guidelines from the National Institute of Standards and Technology, the Canadian Centre for Cyber Security, and the United States Federal Bureau of Investigations in development of this policy, with an intent that such policy can be adopted as best practice for Canadian Municipalities.

SUMMARY OF BACKGROUND

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. This type of cybercrime has been growing and proliferating around the world, and including incidents in Canada. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

According to Media reports, the Town of Midland in Ontario was subject to such an attack last fall. It took weeks to recover computer systems and the Town's insurer negotiated with the attacker on the ransom. Here in Toronto, the Auditor General has reported that two small entities (agencies) within the City were reportedly attacked by ransomware and their systems compromised. Toronto is committed to a formal Cyber-Security program to protect information and manage risk and business continuity.

As chair of General Government and Licensing Committee with the City of Toronto, I am deeply interested in safeguarding Toronto's cybersecurity from this epidemic. The City of Toronto already has a foundation of cyber security measures in place to protect the City's information technology systems. The City is in the process of enhancing our capabilities in a number of areas to address increasingly sophisticated cyber threats. For example, the City is in the process of procuring a Managed Security Services Provider (MSSP) and recruiting a Chief Information Security Officer.

Another one of Toronto's initiatives is to develop incident management procedures and reporting protocols specific to cyber incidents. The City's Information and Technology division has an existing Major Incident Management Procedure in place that is followed when someone contacts the Division's Service Desk to report an incident, any IT-related incident, including a ransomware attack. In addition, staff are preparing supplemental material to address how the City will communicate with other stakeholders outside of Information and Technology division and activate Toronto's Emergency Operations Centre (EOC) in the event of a major cyber-attack. This scenario has never occurred in Toronto, so the City needs to prepare for it.

I recommend staff to develop, for the March 2020 Board meeting, an action plan to advance FCM’s policy on cybersecurity and ransomware, including reference to guidelines from the National Institute of Standards and Technology, the Canadian Centre for Cyber Security, and the United States Federal Bureau of Investigations in developing this policy, with an intent that such policy can be adopted as best practice for Canadian Municipalities.

Submitted by Councillor Paul Ainslie
September 12, 2019