REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Cyber Safety: A Robust Cybersecurity Program Needed to Mitigate Current and Emerging Threats

Date: October 8, 2019
To: Audit Committee
From: Auditor General
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

This report involves the security of property belonging to the City or one of its agencies and corporations.

The attachment to this report contains information explicitly supplied in confidence to the City of Toronto which, if disclosed, could reasonably be expected to impact the safety and security of the City and its services.

SUMMARY

Over the past decade, the City of Toronto, like other large organizations, is increasingly conducting business and key operations online and in a networked environment. This makes operations more efficient and citizens are served better.

The City stores a vast amount of confidential and sensitive data, such as information about employees and citizens' personal records. It also maintains a large number of systems that are critical to the City's functioning, such as water, fire services, transportation, and emergency response systems.

The Canadian Centre for Cyber Security, which is Canada's single unified source of expert advice, guidance and support on cyber security for government, critical infrastructure owners and operations, notes that:

> *"a safe and secure cyber space is important for … security, stability, and prosperity"*

It also assessed that:

> *"Public institutions are also attractive to cyber threat actors* ..."[1]

1 Canadian Centre for Cyber Security, National Cyber Threat Assessment, October 2018

In recent years, many municipalities in Canada and the U.S. have been affected by cyberattacks. Recent attacks on the City of Saskatoon, the City of Ottawa and the City of Burlington are evidence that Canadian cities are targeted.

To improve security considerably, the City must change in three key areas:

- Human behaviour as it relates with cybersecurity threats
- Technical fixes
- Culture shift.

If the City's cybersecurity program is built on these three pillars, cybersecurity will be strengthened considerably.

Auditor General raised concerns in this area before

In previous assessments on information technology security, the Auditor General's reports highlighted to City management that insufficient preparation to manage cyber threats is widely considered to be one of the most critical operational risks facing the organization. The reports are available in Confidential Attachment 1, Appendix 2.

During the Auditor General's most recent follow-up process, management reported that two of the 10 recommendations from information technology security audits done in 2016 were fully implemented. The Auditor General's validation of the implementation of these recommendations found that they were not fully implemented.

These recommendations were considered as not fully implemented because the steps undertaken, or the extent of the improvement did not fully address the issue or the intent of the recommendation. Since 2016 none of the recommendations have been fully implemented, which is concerning to the Auditor General.

The purpose of this audit was to assess the City's ability to manage external and internal cybersecurity threats, and to follow-up on previous audit recommendations. We provided the I&T Division with a detailed technical report to help them understand and address these issues.

This public report contains two administrative recommendations. The confidential audit findings and recommendations to improve cybersecurity controls are presented separately to this report in Confidential Attachment 1. The confidential report will be made public at the discretion of the Auditor General after discussing with appropriate City Official.

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council adopt the confidential recommendations contained in Confidential Attachment 1 to the report (October 8, 2019) from the Auditor General.

2. City Council direct that all information contained in Confidential Attachment 1 to the report from the Auditor General be *released* publicly at the discretion of the Auditor General after discussing with the appropriate City Official.

FINANCIAL IMPACT

Implementing the recommendations in this report will strengthen information technology security controls at the City and at its Agencies and Corporations. The extent of costs and resources needed to implement the recommendations is not determinable at this time. The investments needed to improve controls to manage and respond to cyber threats offsets the potentially significant costs that could result from security breaches, which could include , data recovery/cleanup, financial loss, reputation damage, fines and litigation.

Given the security risks to the City's IT networks, systems and major infrastructure, the Auditor General plans to expedite the audit of IT security systems throughout the City and its major Agencies and Corporations.

DECISION HISTORY

The Auditor General's 2019 Audit Work Plan included a follow-up of the implementation of previous audit recommendations. Considering the importance of cybersecurity with respect to the confidentiality of the City's data, IT network, systems and critical infrastructure, the Auditor General performed this follow-up as a separate project. The Auditor General's 2019 Audit Work Plan is available at:

https://www.toronto.ca/legdocs/mmis/2019/au/bgrd/backgroundfile-124769.pdf

COMMENTS

With cyber threats evolving, there is an urgent need for the City of Toronto to enhance its cybersecurity program to adapt to new threats.

Approximately 4,700 terabytes, comprised of billions of pieces of data, are housed in various systems and computers at the City. A single breach could have a devastating impact on City operations. A system is only as strong as its weakest link.
Increasing cyberattacks, in particular 'Ransomware', across the United States prompted the Department of Homeland Security to issue the following advisory:

"*Ransomware has rapidly emerged as the most visible cybersecurity risk playing out across our nation's networks, locking up private sector organizations and government agencies alike. And that's only what we're seeing – many more infections are going unreported."*[2]

Industry experts on information technology highlight features of the current threat environment:

"*Current attacks are very sophisticated. They're evolving on an almost daily basis."* [3]

"Threats continuously probe for weak points in people, corporations, processes and technologies." [4]

The Canadian Centre for Cyber Security stresses that:

"Information technology security is everyone's responsibility

Inadequate information technology security practices provide cyber threat actors with an easy way to bring down your organization's network and give them access to sensitive information." [5]

What constitutes a cyberattack?

Cyberattacks, meaning unauthorized attempts (successful or not) to gain access to a system and confidential data, modify it in some way, or delete or render information in the system unusable, are one of the biggest threats facing organizations today. The World Economic Forum report on global risks reported "*A large majority of respondents expected increased risks in 2019 of cyber-attacks...*"[6.]

The results of a cyberattack can be devastating. Cities that suffer a cyberattack are subject to the following:

- Inability to fulfil their role of service delivery, which can include critical services like water, fire and emergency services
- Sensitive personal information disclosed
- Supply chain/vendor management relationship interrupted
- Intellectual property theft
- Financial losses
- Risk of legal damages from lawsuits
- Reputational damage

2 Department of Homeland Security – CISA Insights – Ransomware Outbreak, August 21, 2019
3 Standing Committee on Public Safety and National Security-SECU-155 April 3, 2019
4 SECU Committee News Release, June 20, 2019
5 Canadian Centre for Cyber Security, Common Employee IT Security Challenges (ITSAP.00.005)
6 The Global Risks Report 2019 14th Edition – World Economic Forum

Recent cyberattacks on municipalities

In recent years, many municipalities in Canada and the U.S. have been affected by cyberattacks. These attacks have commonly taken two forms — ransomware or phishing by impersonating someone high up in an organization.

In August 2019, the City of Saskatoon revealed that some staff members had sent more than $1 million to a person who was using email to impersonate a Chief Financial Officer for a construction company the City was working with.

In April 2019, the City of Ottawa's Treasurer received an email from what appeared to be the City Manager, asking for funds to be transferred to a new bank account. The treasurer transferred the funds, only to discover that the City Manager's email account had been impersonated, and the money had been transferred to fraudsters.

In June 2019, the City of Burlington faced a similar situation and ended up sending a fraudster more than $500,000.

A recent New York Times article[7] outlined how more than 40 municipalities in the U.S. – including large cities like Baltimore and Atlanta – have been hit by ransomware attacks. Some of these municipalities chose to pay the ransom to unlock data that had been encrypted or to restore access to systems. While others did not pay the ransom because there was no assurance the files/systems would be unlocked. It has cost municipalities millions of dollars to recover from these attacks, in addition to the costs of data clean up and systems recovery.

According to the Canadian Centre for Cyber Security, *"Cyber threat activity against Canadians often has financial or privacy implications. Yet cyber threat activity against*

7 Ransomware Attacks Are Testing Resolve of Cities Across America, August 22, 2019, The New York Times

Canadian businesses and critical infrastructure can have more far-reaching consequences, such as operational disruptions to the financial sector, large-scale theft of personal information, and even potential damage to infrastructure."[8]

With the level of services, extent of personal data, and the critical infrastructure the City supports, the City of Toronto must do all it can to protect its' systems against cyberattacks and to adapt to emerging threats. Opportunities to do this are outlined in the Confidential Attachment 1.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We express our appreciation for the co-operation and assistance we received from management and staff of the I&T Division. We also would like to acknowledge assistance from Toronto Water, Paramedic Services and Fire Services IT staff for their timely provision of requested information, as well as other operating divisions that provided information to us throughout the audit.

CONTACT

Syed Ali, Audit Director, IT & Strategy, Auditor General's Office
Tel: 416-392-8438, Fax: 416-392-3754, email: syed.ali@toronto.ca

Gawah Mark, Senior Audit Manager, Auditor General's Office
Tel: 416-392-8439, Fax: 416-392-3754, email: gawah.mark@toronto.ca

SIGNATURE

Beverly Romeo-Beehler
Auditor General

ATTACHMENTS

Confidential Attachment 1 - Cyber Safety: A Robust Cybersecurity Program Needed to Mitigate Current and Emerging Threats

8 National Cyber Threat Assessment 2018 - Canadian Centre for Cyber Security