REPORT FOR ACTION

Establishment of City Wide Cyber Security Breach Incident Management Procedures Required

Date: June 19, 2019
To: Audit Committee
From: Auditor General
Wards: All

SUMMARY

In our report entitled "Audit of Information Technology Vulnerability and Penetration Testing – Phase 1: External Penetration Testing" we highlighted to the City management that insufficient preparation to manage cyber threats is widely considered as one of the most critical operational risks facing the organizations. The City, as well as its agencies and corporations are not immune from these risks.

The Auditor General recently became aware that two small entities within the City were reportedly attacked by ransomware and their systems compromised.[1] In both situations, the incidents were not communicated to the Chief Information Officer because protocols do not exist.

Ransomware is a form of attack where user systems and/or files become non-operable after the attack. The attackers then demand payment for restoring access to the system and/or files. These attacks are not new to Canadian municipalities; recently, two other municipalities were attacked by ransomware, one in Quebec and one in Ontario. One of the municipalities was demanded $65,000 to restore the data; for the other, the ransom details are not public. Cyber security attacks are increasingly becoming more complicated, difficult to detect and costly for compromised organizations.

The purpose of this report is to highlight the importance and urgency for the City to have a standard incident management process developed and implemented across City divisions, its agencies and corporations so that the Chief Information Officer can analyze these attacks in an effort to enhance City-wide cyber security. The Auditor General, realizing the emerging risks, in each of her reports on IT vulnerability assessments and IT infrastructure audits issued during 2016 to 2018, recommended that the City:

- develop baseline IT security standards to provide guidance across the City to address cyber security threats,

[1] These incidents are still under review.

- implement a cyber security program, and
- create an independent role of the Chief Information Security Officer (CISO).

In addition, the Auditor General, in her communications with the Information and Technology Division, identified the need to have a centralized process, guidelines and communication protocols available to all organizations within the City to deal with cyber security threats and incidents. Adequate controls must be put in place to maintain confidentiality of sensitive information.

The Auditor General's planned follow-up is due in the later half of 2019. An update of the status of the implementation of recommendations will be tabled at future Audit Committee meetings.

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council request the City Manager, the Chief Information Officer and the City Clerk to coordinate and develop standard incident management procedures including communication protocols to address incidents involving cyber attacks/information breaches. The procedures and protocols should include:

    (a) Guidelines describing the sequence of actions that should take place as soon as staff become aware of a cyber attack/information breach incident

    (b) Communication protocols detailing key contact names, functions and contact information for staff to receive guidance

    (c) Reports to be completed by the affected organization, detailing the date of incident, systems affected, information compromised, and other relevant details

    (d) Communications to the media/public, where required, including privacy protocols.

The incident management procedures and communication protocols should be liaised across the City, including agencies and corporations.

FINANCIAL IMPACT

The recommendation in this report has no financial impact. However, preventing cyber security attacks would save the City from significant costs that could potentially result from security breaches, such as data clean-up and system restore costs, statutory fines and litigation.

DECISION HISTORY

The Auditor General has a mandate to advise Council of potential risks and threats to the organization. In line with this duty, the Auditor General has issued the following reports concerning information technology management and security. The reports are available at:

(i) Audit of Information Technology Vulnerability and Penetration Testing – Phase 1: External Penetration Testing, February 2016
https://www.toronto.ca/legdocs/mmis/2016/au/bgrd/backgroundfile-90751.pdf

(ii) Audit of Information Technology Vulnerability and Penetration Testing – Phase II: Internal Penetration Testing, Part 1 – Accessibility of Network and Servers, October 2016
https://www.toronto.ca/legdocs/mmis/2016/au/bgrd/backgroundfile-97617.pdf

(iii) Information Technology Vulnerability Assessment and Penetration Testing - Wrap-up of Phase I and Phase II, March 2017
https://www.toronto.ca/legdocs/mmis/2017/au/bgrd/backgroundfile-101892.pdf

(iv) IT Infrastructure and IT Asset Management Review: Phase 1: Establishing an Information Technology Roadmap to Guide the Way Forward for Infrastructure and Asset Management, January 2018
https://www.toronto.ca/legdocs/mmis/2018/au/bgrd/backgroundfile-112385.pdf

(v) Information Technology Infrastructure and Asset Management Review: Phase 2: Establishing Processes for Improved Due Diligence, Monitoring and Reporting for Effective IT Projects and Asset Management, June 2018
https://www.toronto.ca/legdocs/mmis/2018/au/bgrd/backgroundfile-118363.pdf

COMMENTS

The City is legislatively obligated to protect personal information under the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) or the *Personal Health Information Protection Act* (PHIPA) (the Acts).

The cyber security attacks are not new to Canadian municipalities and other public and private sector organizations. Recently, two municipalities were attacked by ransomware. One of the municipalities was demanded $65,000 to restore the data; for the other, the ransom details are not public.

Quebec's Regional Municipality Ransomware Attack
https://www.ctvnews.ca/canada/quebec-region-pays-30-000-bitcoin-ransom-after-servers-hacked-1.4182012

City of Stratford, Ontario Ransomware Attack
https://www.cbc.ca/news/politics/stratford-cyberattack-ransomware-hack-1.5170951

It is important to have adequate prevention, detection and remedial procedures in place across the City, including agencies and corporations, to effectively deal with any form of cyberattack or data breach in a coordinated fashion.

Most City agencies and corporations are separate institutions under MFIPPA and have their own designated leader in charge of privacy. The Auditor General encourages the City and its agencies and corporations to coordinate how these incidents should be reported and handled.

CONTACT

Ina Chan, Assistant Auditor General, Auditor General's Office
Tel: 416-392-8472; Fax: 416-392-3754; E-mail: ina.chan@toronto.ca

Syed Ali, Audit Director, Auditor General's Office
Tel: 416-392-8438; Fax: 416-392-3754; E-mail: Syed.Ali@toronto.ca

SIGNATURE

Beverly Romeo-Beehler
Auditor General