REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Auditor General's Cybersecurity Review: Open-Source Internet Data Intelligence Review

Date: May 20, 2022
To: Audit Committee
From: Auditor General
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

The Confidential Attachment 1 to this report involves the security of the property of the City of Toronto and its agencies and corporations.

SUMMARY

Cyber threats are on the rise and continue to evolve. Many municipalities in Canada and the U.S. have been affected by cyberattacks in recent years. The Toronto Transit Commission was recently hit by a ransomware attack in October 2021.[1]

In Canada, the estimated average cost of a data breach is $6.35 million.[2] As cybersecurity threats expand and become more complex, the Auditor General continues to proactively examine the controls and evolving cyber threats to the City, its agencies and corporations, and make recommendations to improve cybersecurity.

Cyber attackers leverage the data available over the internet for an organization and its staff to launch cyberattacks. It is important that the data available over the internet is monitored, and actions are taken to reduce the cyberattack surface. We used Open-Source Intelligence (OSINT) gathering for data available on the internet to perform this review.

The objective of this review was to identify information available over the internet that may present cybersecurity risks to the City and its agencies and corporations. The organizations reviewed included:

1 Cybersecurity incident (ttc.ca)

2 Cyber threat bulletin: The ransomware threat in 2021 - Canadian Centre for Cyber Security

- City of Toronto
- Toronto Police Service
- Toronto Public Library
- Toronto Transit Commission (TTC)
- Toronto Hydro

This report contains two recommendations. The confidential findings and recommendations from our review are contained in the Confidential Attachment 1 to this report.

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council adopt the confidential instructions to staff in Confidential Attachment 1 to this report from the Auditor General.

2. City Council direct that Confidential Attachment 1 to this report from the Auditor General be released publicly at the discretion of the Auditor General, after discussions with the appropriate officials at the City and its agencies and corporations.

FINANCIAL IMPACT

Implementing the cybersecurity review recommendations will strengthen cybersecurity controls at the City and its agencies and corporations. The extent of costs and resources needed to implement the recommendations is not determinable at this time. The investment 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, reputational damage, fines or litigation.

DECISION HISTORY

Given the rapidly evolving cyber threats, the Auditor General has included cybersecurity audits in her Annual Work Plans on an ongoing basis for past number of years. The Auditor General's Office work plans from 2019 to 2022 are available at:

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

https://www.toronto.ca/legdocs/mmis/2019/au/bgrd/backgroundfile-138873.pdf

https://www.toronto.ca/legdocs/mmis/2020/au/bgrd/backgroundfile-158178.pdf

https://www.toronto.ca/legdocs/mmis/2021/au/bgrd/backgroundfile-172597.pdf

In 2021, the Auditor General completed a review of selected critical systems at Toronto Fire Services (TFS). This OSINT review is an extension of work completed at TFS and was expanded to include all City divisions and its major agencies and corporations.

COMMENTS

There have been incidents where cyber attackers utilized organizations' available information on the internet to attack them. The 2021 high-profile cyber incident that disabled the largest fuel pipeline network in the U.S. was reportedly the result of a single compromised password that was discovered on the Dark Web.

“Hackers gained entry into the networks… through a Virtual Private Network account… The account’s password has since been discovered inside a batch of leaked passwords on the Dark Web. That means a Colonial employee may have used the same password on another account that was previously hacked.” [3]

Although an online presence is essential for organizations to conduct business, it is also important that digital footprints are managed and secured. It requires continuous vigilance over the IT perimeter and the digital footprint the organization has over the internet. The Canadian Centre for Cyber Security describes digital footprints as:

"A digital footprint is the trail of data you create while using the Internet. This trail of data comes from the websites you visit, the emails you send, and the information you submit or download online." [4]

Confidential Attachment 1 to this report contains five recommendations to improve cybersecurity across the City and its agencies and corporations. The Auditor General will perform a follow-up review after management has implemented the recommendations.

The procedures and work performed for this report do not constitute an audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). However, we believe the work performed and information gathered provide a reasonable basis for our findings, conclusions and recommendations.

We express our appreciation for the co-operation and assistance we received from the management and staff at the City and its agencies and corporations. The timely provision of information and coordination of various activities by the designated team has greatly helped us to complete this review.

3 Hackers breached Colonial Pipeline using compromised password - BNN Bloomberg

4 Digital footprint (ITSAP.00.133) - Canadian Centre for Cyber Security

CONTACT

Syed Ali, Assistant Auditor General (A), IT and Strategy, Auditor General's Office
Tel: 416-392-8438, Fax: 416-392-3754, E-mail: Syed.Ali@toronto.ca

Cecilia Jiang, Senior Audit Manager, Auditor General's Office
Tel: 416-392-8024, Fax 416-392-3754, E-mail: Cecilia.Jiang@toronto.ca

SIGNATURE

Beverly Romeo-Beehler
Auditor General

ATTACHMENTS

Confidential Attachment 1: Auditor General’s Cybersecurity Review: Open-Source Internet Data Intelligence Review