For Action

Toronto Transit Commission Cybersecurity Audit Phase 1: Critical IT Assets and User Access Management

Date: April 14, 2022
To: TTC Board

Reason for Confidential Information

This report contains information related to the security of the property of the municipality or local board.

Summary

The subject report was reviewed by the TTC Audit & Risk Management Committee on March 31, 2022 and is forwarded to the TTC Board for its consideration.

Recommendations

It is recommended that the TTC Board:

1. The Toronto Transit Commission Board adopt the confidential instructions to staff in Confidential Attachment 1 to this report from the Auditor General.

2. The Toronto Transit Commission Board forward this report to City Council for information through the City's Audit Committee.

3. The Toronto Transit Commission Board 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 Toronto Transit Commission and City Officials.

Attachments

Attachment 1 – Toronto Transit Commission Cybersecurity Audit Phase 1: Critical IT Assets and User Access Management

REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Toronto Transit Commission Cybersecurity Audit Phase 1: Critical IT Assets and User Access Management

Date: March 22, 2022
To: TTC Audit and Risk Management Committee
From: Auditor General
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

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

SUMMARY

Cyberattacks are widely considered to be one of the most critical operational risks facing organizations. According to the Canadian Centre for Cyber Security Bulletin, 2021[1]:

"2021 has been marred by a series of high-profile ransomware attacks around the world... In the first half of 2021, global ransomware attacks increased by 151% when compared with the first half of 2020. This year has also been marked by the highest ransoms and the highest payouts. In Canada, the estimated average cost of a data breach, a compromise that includes but is not limited to ransomware, is $6.35M CAD. The Cyber Centre has knowledge of 235 ransomware incidents against Canadian victims from 1 January to 16 November 2021. More than half of these victims were critical infrastructure providers."

Cybersecurity threats to the City are real. Cyber attackers recently attacked Toronto Transit Commission's (TTC) IT infrastructure. The attack affected several critical services, including Vision (a critical application used to communicate with vehicle operators), Wheel-Trans (a critical reservation application), and TTC's internal email

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

service. The personal information of 25,000 current and former TTC employees may also have been stolen during the attack[2].

The Auditor General has been proactive in her audits of cybersecurity at the City and has completed several vulnerability assessments and penetration testing of critical systems at the City, including an overall assessment of the City's IT infrastructure, Toronto Water SCADA system, Fire Services critical system and Toronto Police IT infrastructure. Cybersecurity reviews are now expanding to include agencies and corporations.

The Auditor General initiated a cybersecurity audit of the TTC in accordance with her 2021 Work Plan. The planning for this audit was underway when the TTC became a victim of a ransomware attack on October 29, 2021. However, the Auditor General's testing team had already gathered some information about the TTC's IT systems and infrastructure, and she was able to continue with her work. The phase 1 report contains the results of this part of her assessment, so that management can address the vulnerabilities found in a timely manner.

This report includes the results of our review of critical IT assets and processes used to manage IT system users at TTC. We will provide future reports after completing the next series of audits, which were temporarily suspended so that TTC could focus on restoring services and systems affected by the October 2021 cyber attack.

This report contains three administrative recommendations. The confidential findings and recommendations from our audit are contained in Confidential Attachment 1.

RECOMMENDATIONS

The Auditor General recommends that:

1. The Toronto Transit Commission Board adopt the confidential instructions to staff in Confidential Attachment 1 to this report from the Auditor General.

2. The Toronto Transit Commission Board forward this report to City Council for information through the City's Audit Committee.

3. The Toronto Transit Commission Board 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 Toronto Transit Commission and City Officials.

2 Cybersecurity incident (ttc.ca)

FINANCIAL IMPACT

Implementing the cybersecurity audit recommendations will strengthen cybersecurity controls at the TTC. 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

The Auditor General has conducted several cybersecurity audits at the City. Her 2021 Work Plan included cybersecurity audits of the City's critical infrastructure as well as its agencies and corporations. The Auditor General's 2021 Work Plan included TTC's IT infrastructure cybersecurity audit and is available at:

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

COMMENTS

Cyberattacks on governments and critical infrastructure providers are on the rise. Recent cyberattacks on public transit systems in Toronto, Vancouver and Montreal are a clear indication of this rising threat[3].

Cyberattacks are 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. As cybersecurity threats expand and evolve, it is important that the Auditor General continue her work on cybersecurity so that she can make recommendations to improve security controls.

The TTC is a public transit agency that provides essential services to millions of Torontonians. It is the largest public transit system in Canada and the third largest in North America.

In her TTC Cybersecurity Audit Phase 1, the Auditor General has made six confidential recommendations in Confidential Attachment 1. The Auditor General will re-test cybersecurity controls after management has implemented the recommendations.

3 Cybersecurity incident (ttc.ca)

Metro Vancouver's transit system hit by ransomware attack | Globalnews.ca

Hackers asked TransLink for $7.5 million in December ransomware attack | CTV News

Hackers demanded $3.7 million in Montreal transit authority 'ransom'; STM says it won't pay | CTV News

The STM completes cyber attack investigation | Société de transport de Montréal

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.

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

Beverly Romeo-Beehler
Auditor General

ATTACHMENTS

Confidential Attachment 1: Toronto Transit Commission Cybersecurity Audit Phase 1: Critical IT Assets and User Access Management