REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Toronto Transit Commission Cybersecurity Audit - Phase Two: Overall Network Security and Cybersecurity Assessment of Select Critical Systems

Date: November 6, 2023
To: Toronto Transit Commission 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

Toronto Transit Commission (TTC) is a public transit agency that provides an average of 1.1 million rides per day on its transit system. Pre-pandemic there were 1.7 million average daily rides. It is the largest public transit system in Canada and the third largest in North America[1].

Canadian Cyber Centre in its 'National Threat Assessment 2023-2024' has identified the transportation sector as a critical infrastructure sector that is increasingly at risk from cyber threat activity.

According to the Canadian Cyber Centre National Cyber Threat Assessment[2]:

"Critical infrastructure is still a prime target for both cybercriminals and state-sponsored actors alike."

"…Ransomware is a persistent threat to Canadian organizations… Critical infrastructure is increasingly at risk from cyber threat activity…" and "Cybercriminals deploying ransomware... will continue to adapt their methods to maximize profits…"

Information technology plays a vital role in all aspects of TTC operations. In 2021, TTC became a victim of a ransomware cyber-attack. Cyber attackers affected several

1 August 2023 TTC CEO report

2 https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf

computer systems and critical services, including the VISION[3] system that is used to communicate with vehicle operators, online Wheel Transit bookings, and TTC's internal email service[4].

Cyber-attacks on Public Transit Systems in North America

According to the Washington Post article published on May 19, 2023, a former contractor for the Washington Metropolitan Area Transit Authority (WMATA) managed to log in and access critical and sensitive WMATA systems from overseas, despite the termination of this individual's contract[5].

The article also cited other cybersecurity incidents on transit systems, such as:

- A ransomware gang said this year that it exposed stolen data from San Francisco's Bay Area Rapid Transit.
- Two years ago, hackers hit both New York's Metropolitan Transit Authority and the Toronto Transit Commission.
- In 2020, ransomware struck Vancouver's TransLink, leading to the disabling of its payment systems. That caused issues for some riders. The hackers also accessed employees' sensitive personal information, and TransLink lost its communications systems.
- Also in 2020, hackers hit the Southeastern Pennsylvania Transportation Authority with a ransomware attack.

Cyber attacks continue to occur on public sector organizations. More recently, Toronto Public Library became victim of a cybersecurity attack. CityNews Toronto in its November 2, 2023 newscast reported the following:

"The Toronto Public Library (TPL) continues to deal with a cybersecurity incident that came to its attention last weekend.

The TPL website remains down, and online services such as "Your account," digital collections, computers and printers at branches are out of service."[6]

The Auditor General has been proactive in her audits of cybersecurity and has completed several vulnerability assessments and penetration testing of critical systems at the City, and its agencies and corporations. In March 2022, the Auditor General completed the phase 1 audit on critical IT assets and processes used to manage IT system users at TTC. The public report is available at:

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

3 Vehicle Information System & Integrated Operations Network

4 https://globalnews.ca/news/8358094/ttc-cyber-attack-investigation-employee-information/

5 A cyber scare for public transit

6 https://toronto.citynews.ca/2023/11/02/toronto-public-library-cybersecurity-ransomware/

This Phase 2 report includes the results of our cybersecurity audit of TTC's IT network, systems and applications. The report contains three administrative recommendations and nine confidential recommendations. The confidential findings and recommendations are contained in Confidential Attachment 1 to this report. The Auditor General will re-test cybersecurity controls after management has implemented the recommendations.

RECOMMENDATIONS

The Auditor General recommends that:

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

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

3. The Board recommend City Council authorize the public release of Confidential Attachment 1 to the report from the Auditor General at the discretion of the Auditor General, after discussions with the appropriate Toronto Transit Commission and City Officials.

FINANCIAL IMPACT

Implementing the audit recommendations will strengthen cybersecurity controls at 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's 2023 Work Plan included TTC's IT infrastructure cybersecurity audit and is available at:

https://www.toronto.ca/legdocs/mmis/2023/au/bgrd/backgroundfile-234051.pdf

COMMENTS

What is a cyberattack?

The National Institute of Standards and Technology (NIST) defines a cyberattack as:

"Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself"[7].

Cyber Threats on Government Services and Critical Infrastructure

Cyberattacks on governments and critical infrastructure providers are a significant threat. Earlier in 2023, the Minister of National Defence issued a statement on cyber threats to critical infrastructure, stating[8]**:**

"… Canadian organizations and critical infrastructure operators – who operate the systems on which we depend every day – must be prepared to protect against known cyber threats…", and

"… I urge Canadian critical infrastructure organizations to review the Cyber Centre's Cyber Threat Bulletin: Cyber Threats to Operational Technology".

In September 2023, the Canada's border control agency was the latest federal department to confirm it was hit by a recent wave of denial-of-service attacks, as reported in a news article published on September 20, 2023[9].

"The Canada Border Services Agency (CBSA) can confirm that connectivity issues that affected kiosks and electronic gates at airports on Sunday, September 17, 2023 are the result of a distributed denial of service attack campaign (DDoS)[10]*, recently targeting several Canadian sectors"*

TTC is a large city organization providing essential services. It has a vast network of buses, streetcars, and subways. Figure 1 provides some operating statistics about TTC[11].

7 https://csrc.nist.gov/glossary/term/Cyber_Attack

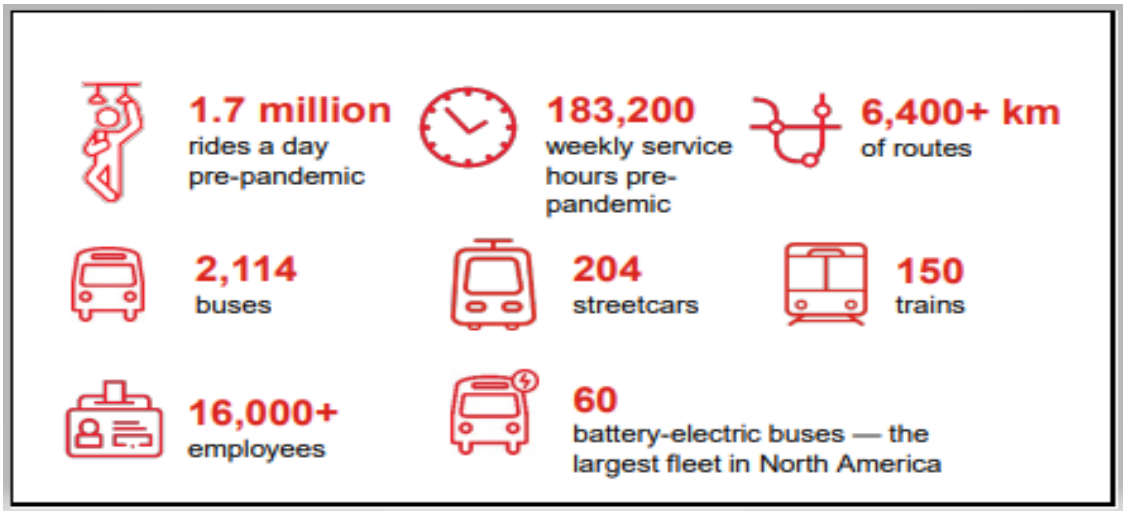
8 https://www.canada.ca/en/communications-security/news/2023/04/statement-from-the-minister-of-national-defence--cyber-threats-to-critical-infrastructure.html

9 https://financialpost.com/technology/ddos-attacks-behind-canada-border-agency-problems

10 This type of attack prevents users from accessing connected online services and websites.

11 August 2023 CEO's Report Cover (azureedge.net)

Figure 1: TTC by the numbers



Information technology plays a critical role in all aspects of TTC operations. 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 across the City, and its agencies and corporations.

The phase 2 audit focused on TTC's IT network security, systems and applications. The Auditor General has made nine confidential recommendations in 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.

CONTACT

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

Gawah Mark, Audit Director, Auditor General's Office
Tel: (416) 392-8439, E-mail: Gawah.Mark@toronto.ca

Andrew Krupowicz, Senior Audit Manager, Auditor General's Office
Tel: (416) 392-3703, E-mail: Andrew.Krupowicz@toronto.ca

SIGNATURE

Tara Anderson
Auditor General

ATTACHMENTS

Confidential Attachment 1: Toronto Transit Commission Cybersecurity Audit - Phase Two: Overall Network Security and Cybersecurity Assessment of Select Critical Systems