TORONTO

REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Cybersecurity Audit of Toronto Public Library: Overall Assessment of Network, Systems and Physical Security

Date: May 15, 2026
To: Toronto Public Library Board
From: Auditor General
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

Confidential Attachments 1 and 2 to this report involve the security of the property of the City of Toronto or one of its agencies and corporations.

SUMMARY

The Toronto Public Library (TPL) operates the largest public library system in Canada through TPL's network of 100 branches across Toronto. In 2024, there were 13.4 million in-branch visits and 31.5 million online visits, with approximately 1.1 million registered library cardholders.[1] The TPL's 2025 operating budget was $269 million, funded mostly by the City of Toronto along with fees, and other revenue sources.[2]

Technology plays an important role in all aspects of the TPL's operations. This report includes the results of our vulnerability assessment and penetration testing of the TPL's network, systems, applications and devices. We also reviewed user access management, cybersecurity incident logging and monitoring, and tested physical security in relation to cybersecurity.

This report includes three administrative recommendations. The confidential findings and recommendations are contained in **Confidential Attachment 1** to this report. A separate confidential technical report has been provided to management with technical details to guide them in addressing the report findings and recommendations.

1 TPL 2024 Public Service Statistics, Trends & Comparisons, pages 2, 23 & 32

2 Toronto Public Library - 2025 Budget Presentation, page 10

Management agrees with the recommendations in the Confidential Attachment 1, which also includes management's response.

RECOMMENDATIONS

The Auditor General recommends that:

1. The Board receive the public report and Confidential Attachments 1 and 2 from the Auditor General.

2. The Board direct that all information contained in Confidential Attachments 1 and 2 to this report remain confidential.

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

FINANCIAL IMPACT

Implementing the audit recommendations contained in **Confidential Attachment 1** will further strengthen cybersecurity controls at the Toronto Public Library. 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 potential costs resulting from security breaches, which could include data recovery/cleanup, financial loss, reputational damage, fines, or litigation.

DECISION HISTORY

The Auditor General's 2025 Work Plan included a vulnerability assessment and penetration testing of Toronto Public Library's information and technology infrastructure, networks, and systems to assess cybersecurity risks and controls. The Auditor General's 2025 Work Plan is available at:

Auditor General's Office 2025 Work Plan and Budget Highlights

COMMENTS

Cybersecurity threats continue to grow in frequency and sophistication. The Canadian Centre for Cyber Security 2025-2026 National Cyber Threat Assessment report noted that:

"Canada is confronting an expanding and complex cyber threat landscape with a growing cast of malicious and unpredictable state and non-state cyber threat actors…that are targeting our critical infrastructure and endangering our national

security. These cyber threat actors are evolving their tradecraft, adopting new technologies, and collaborating in an attempt to improve and amplify their malicious activities." [3]

Recent Cyberattacks on Public Library Systems

- Toronto Public Library was affected by a cyberattack in October 2023 that disrupted systems and online services across its library branches.[4]

- British Library of the United Kingdom experienced a ransomware attack in October 2023 on its infrastructure affecting systems and data.[5]

- Seattle Public Library was targeted by a ransomware attack in May 2024, disrupting access to staff and public computers, various internal systems, and the library's website.[6]

Since 2015, the Auditor General has proactively audited cybersecurity at the City and has completed several vulnerability assessments and penetration testing of critical systems at the City, and its agencies and corporations. With cybersecurity threats evolving across the globe, the City of Toronto and its agencies and corporations must ensure their cybersecurity programs are adapting to new challenges and threats.

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.

The Auditor General will retest cybersecurity controls at the TPL after management has fully implemented the recommendations.

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

Suzanna Chan, Senior Audit Manager, Auditor General's Office
Tel: (416) 392-8033, E-mail: Suzanna.Chan@toronto.ca

3 Canadian Centre for Cyber Security National Cyber Threat Assessment 2025-2026

4 https://www.libraryjournal.com/story/toronto-public-library-recovers-from-ransomware-attack

5 Lessons learned from the ransomware attack on the British library

6 Why did ransomware hackers target Seattle public library

SIGNATURE

Tara Anderson
Auditor General

ATTACHMENTS

Confidential Attachment 1: Cybersecurity Audit of Toronto Public Library: Overall Assessment of Network, Systems and Physical Security

Confidential Attachment 2: Confidential Presentation to the Toronto Public Library Board