TORONTO

REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Cybersecurity Audit of Exhibition Place – Phase Two: Overall Network Security and Cybersecurity Assessment of Select Critical Systems

Date: March 25, 2026
To: Board of Governors of Exhibition Place
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 Auditor General included a cybersecurity audit of Exhibition Place, an agency of the City of Toronto, in her 2025 Work Plan. Exhibition Place is Canada's largest convention centre and entertainment and sports venue, generating $595 million[1] in economic impact annually and $67.3 million in revenue in 2024.

Phase One of this cybersecurity audit was presented at Exhibition Place's December 5, 2025, Board meeting. The Auditor General's Phase One confidential report included results from testing physical security, user access management, and staff awareness of social engineering in relation to cybersecurity. The Phase One public cover report is available at:

Cybersecurity Audit of Exhibition Place – Phase One: Physical Security, User Access Management and Staff Training

Technology plays a vital role in all aspects of Exhibition Place's operations and services. This Phase Two report includes the results of our vulnerability assessment and penetration testing of the Exhibition Place's network, systems, applications and devices, as well as cybersecurity incident logging and monitoring review.

1 Budget TO 2026 Budget Notes Exhibition Place

This report includes five administrative recommendations. The confidential findings and recommendations are contained in Confidential Attachment 1 to this report. A separate, confidential and detailed technical report was provided to management with technical details to guide them in addressing the report findings and recommendations.

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

RECOMMENDATIONS

The Auditor General recommends that the Board of Governors of Exhibition Place:

1. Adopt the Confidential Recommendations in Confidential Attachment 1.

2. Subject to City Council approval, direct that Confidential Attachment 1 be released at the discretion of the Auditor General, after discussions with the appropriate Exhibition Place and City officials.

3. Direct the Confidential Attachment 2 remain confidential in its entirety, as it pertains to the security of the property of the City of Toronto or one of its agencies and corporations.

4. Forward this report and Confidential Attachment 1 to City Council for information through the City's Audit Committee.

5. Recommend that City Council authorize the public release of Confidential Attachment 1 at the discretion of the Auditor General, after discussions with the appropriate Exhibition Place and City officials.

FINANCIAL IMPACT

Implementing the audit recommendations contained in Confidential Attachment 1 will further strengthen cybersecurity controls at the Exhibition Place. 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 cybersecurity audit of a selected agency's overall network security and critical systems, and Exhibition Place was selected as the agency for this audit. The Auditor General's 2025 Work Plan is available at:
Auditor General's Office 2025 Work Plan and Budget Highlights

COMMENTS

Cybersecurity threats are constantly evolving and becoming more complex. The Canadian Centre for Cyber Security's National Cyber Threat Assessment 2025-2026 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." [2]

Recent cyberattacks targeting the public sector

Cities have also become targets of cyberattacks in recent years:

- Toronto Public Library – the library experienced a significant cyberattack in October 2023 that disrupted systems and online services across its library branches.[3]
- Toronto Zoo – in an early 2024 cyber incident, current, former, and retired employees had personal information stolen.[4]
- City of Hamilton – in February 2024 the City of Hamilton was the victim of a ransomware attack that impacted city systems and disrupted municipal services.[5]

Since 2015, the Auditor General has proactively audited cybersecurity 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 Exhibition Place after management fully implements the recommendations.

2 National Cyber Threat Assessment 2025-2026

3 Library Journal Toronto Public Library Ransomware Attack

4 Toronto Zoo Cyber Incident

5 City of Hamilton Cybersecurity Update-Release of Incident Impact Report

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

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

SIGNATURE

Tara Anderson
Auditor General

ATTACHMENTS

Confidential Attachment 1: Cybersecurity Audit of Exhibition Place – Phase Two: Overall Network Security and Cybersecurity Assessment of Select Critical Systems

Confidential Attachment 2: Confidential Presentation to the Board of Governors of Exhibition Place