REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

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

Date: November 21, 2025
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 Exhibition Place is an agency of the City of Toronto and managed by the Board of Governors of Exhibition Place. As Canada's largest exhibition and convention centre, the Exhibition Place is used for conventions, conferences, trade shows, entertainment and sporting events, public celebrations, festivals, and cultural attractions, generating over $594.5 million per year in economic impact.[1]

Technology plays a vital role in all aspects of the Exhibition Place's operations and services. Given the size of the operations, and the services that Exhibition Place provides, the Auditor General included a cybersecurity audit of the Exhibition Place in her 2025 Work Plan.

This audit is conducted in two phases. Phase One of this audit focused on:

- Physical security at selected facilities,
- User access management, and
- Social engineering and staff awareness.

[1] 2025 Capital and Operating Budget Notes – Exhibition Place, page 6, 7th. bullet point.

Phase Two, which is in progress, will include an overall assessment of Exhibition Place's networks, systems, and application security and will be reported to the Board in April 2026.

This report includes five administrative recommendations. The confidential findings and recommendations are contained in Confidential Attachment 1 to this report. A separate confidential detailed technical report has been 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

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. Over the past few years, there has been an increase of cyberattacks on the City's agencies, such as the Toronto Zoo, Toronto Public Library, and Toronto Transit Commission.

The Auditor General has conducted cybersecurity audits at the City and its agencies and corporations since 2015 and included a cybersecurity audit of the Exhibition Place in her 2025 Work Plan. This Phase One cybersecurity audit focused on the assessment of physical security, user access management, and staff awareness related to social engineering.

Physical Security

Physical security can prevent an unauthorized person from gaining direct access to an organization's facilities. This provides an essential layer of defence by protecting critical IT assets and computer systems from being exploited or sabotaged by a malicious actor.

User Access Management

User access controls are important in the overall management of cybersecurity. The Active Directory provides centralized authentication and authorization for network resources. It also manages users and network permissions, such as creating and deleting user accounts and providing access permissions to network resources.

An example demonstrating the importance of user access management is the large-scale and sophisticated "SolarWinds" cyberattack. The Active Directory played a part in this large-scale cyberattack. The attack was initiated through malware inserted into a software update which affected multiple US government agencies, critical infrastructure entities, and private sector organizations in 2020.[2] Research from industry experts found that attackers used the Active Directory to move laterally within the organization.

[2] Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise | CISA

Staff Training – Social Engineering

According to the Canadian Centre for Cyber Security, social engineering attacks are referred to as "human hacking" because threat actors leverage information they have found on the Internet and social media platforms to target an individual or organization. Threat actors lure or trick users into disclosing information about their accounts, passwords, and even system access. Increasing staff awareness through enhanced training can provide another layer of defence as cyber threats evolve and become more sophisticated.

Some examples of social engineering attacks include phishing, quishing, and vishing.[3] Phishing emails are a common initial access point for ransomware attacks[4], and these risks are further elevated using evolving technologies, such as artificial intelligence.

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.

We express our appreciation for the co-operation and assistance we received from the Exhibition Place management and staff.

The Auditor General will retest cybersecurity controls at the Exhibition Place after management fully implements 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

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

SIGNATURE

Tara Anderson
Auditor General

[3] Social engineering – ITSAP.00.166 - Canadian Centre for Cyber Security

[4] Baseline cyber threat assessment: Cybercrime - Canadian Centre for Cyber Security

ATTACHMENTS

Confidential Attachment 1: Cybersecurity Audit of Exhibition Place – Phase One: Physical Security, User Access Management and Staff Training

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