TORONTO Decisions

City Council

Executive Committee - Meeting 14

EX14.3	ACTION	Adopted		Ward: All

Extending the Mandate of the City's Chief Information Security Officer

City Council Decision

City Council on May 22 and 23, 2024, adopted the following:

1. City Council direct the Chief Information Security Officer to establish a cyber security risk management partnership with agencies and corporations by:

a. incorporating their identified cyber risks into the City's governance and compliance risk management program;

b. conducting ongoing cyber security assessments on agencies and corporations;

c. assessing rates of compliance; and

d. developing remediation plans and strategies to reduce risk and promote compliance.

2. City Council direct the following Agencies, and as Shareholder direct the following corporations, in collaboration with the Chief Information Security Officer, to formulate organizational cyber security frameworks aligned with:

a. overarching City cyber security objectives;

b. established international cyber security standards including International Organization for Standardization ISO 27001, Statement on Standards for Attestation Engagement, the International Society of Automation / the International Electrotechnical Commission, National Institute of Standards and Technology NIST 800-171 and NIST 800-171A, and the Payment Card Industry Data Security Standard; and

c. the City's Digital Infrastructure Strategic Framework;

City of Toronto Agencies:

CreateTO;
Exhibition Place;
Heritage Toronto;
TOLive;
Toronto Atmospheric Fund;
Toronto Investment Board;
Toronto Parking Authority;
Toronto Zoo;

Yonge-Dundas Square;
Toronto Transit Commission;

George Bell Arena;
Larry Grossman Forest Hill Arena;
Leaside Memorial Community Gardens Arena;
McCormick Playground Arena;
Moss Park Arena;
North Toronto Memorial Arena;
Ted Reeve Community Arena;
William H. Bolton Arena;

519 Church St Community Centre;
Applegrove Community Complex;
Cecil Community Centre;
Central Eglinton Community Centre;
Community Centre 55;
Eastview Neighbourhood Community Centre;
Ralph Thornton Community Centre;
Scadding Court Community Centre;
Swansea Town Hall Community Centre;
Waterfront Neighbourhood Centre;

City of Toronto Corporations:

Build Toronto Corporation;
Casa Loma Corporation;
Lakeshore Arena Corporation;
Toronto Community Housing Corporation;
Toronto Hydro Corporation;
Toronto Port Lands Company;
Toronto Seniors Housing Corporation.

3. City Council direct the Boards of the Agencies, and as Shareholder direct the Boards of the Corporations set out in Part 2 above to:

a. provide the necessary information, access, and visibility into their cyber security programs to facilitate the cyber security risk management partnership with the Chief Information Security Officer;

b. operationalize the Chief Information Security Officer's recommendations to mitigate cyber risks identified in the cyber security risk management partnership; and

c. engage in consultation with the Chief Information Security Officer on all initiatives that could potentially affect cyber security, including but not limited to rates of compliance, remediation plans and strategies aimed at reducing risks and promoting compliance.

4. City Council request the following Agencies, in collaboration with the Chief Information Security Officer, to formulate organizational cyber security frameworks aligned with:

a. overarching City cyber security objectives;

b. established international cyber security standards including International Organization for Standardization, Statement on Standards for Attestation Engagement, the International

Society of Automation/the International Electrotechnical Commission, National Institute of Standards and Technology, and the Payment Card Industry Data Security Standard; and

c. the City's Digital Infrastructure Strategic Framework

City of Toronto Agencies:

Toronto and Region Conservation Authority;
Toronto Pan Am Sports Centre;
Toronto Police Service;
Toronto Public Library;
Waterfront Toronto.

5. City Council request the Agencies set out in Part 4 above to provide the necessary information, access and visibility into their cyber security programs to facilitate the cyber security risk management partnership with the Chief Information Security Officer.

6. City Council request the Agencies set out in Part 4 above to operationalize the Chief Information Security Officer's recommendations to mitigate identified risks identified in the cyber security risk management partnership.

7. City Council request the Agencies set out in Part 4 above to engage in consultation with the Chief Information Security Officer on all initiatives that could potentially affect cyber security, including but not limited to rates of compliance, remediation plans and strategies aimed at reducing risks and promoting compliance.

8. City Council forward the report (April 30, 2024) from the Chief Information Security Officer to the following Boards for their review of the issues and recommendations and consider the relevance to their respective organizations for implementation appropriate to their governance structure:

Partnered Boards (Shared Governance):

Toronto and Region Conservation Authority;
Waterfront Toronto;
Toronto Pan Am Sports Centre Corporation.

9. City Council direct the Agencies listed in Part 2 above and, as a Shareholder direct the corporations listed in Part 2 above and request the Agencies listed in Part 4 above to engage with the Chief Information Security Officer in the event of a cyber security incident or data breach affecting the agency or corporation, and to work with the Chief Information Security Officer to contain, mitigate and resolve the cyber security incident or data breach.

10. City Council direct the Chief Information Security Officer to engage with the Boards of the Agencies and Corporations on an as-needed basis to facilitate City Council's decision.

11. City Council direct the Chief Information Security Officer to report on specific responses and compliance rates of each Agency and Corporation on an annual basis in October of each year to the Executive Committee.

12. City Council direct the Chief Information Security Officer to report on instances of non-compliance with the above directives or requests to the Executive Committee as often as needed.

13. City Council direct that Confidential Attachment 1 to the report (April 30, 2024) from the Chief Information Security Officer remain confidential in its entirety.

Confidential Attachment 1 to the report (April 30, 2024) from the Chief Information Security Officer remains confidential in its entirety in accordance with the provisions of the City of Toronto Act, 2006, as it pertains to the security of property belonging to the City of Toronto and its agencies and corporations.

Summary

This report responds to a request from City Council for the Chief Information Security Officer to report on the progress of developing an implementation plan for an independent and centralized information technology risk and compliance, privacy, and cyber security function, as per item #15 of 2021.AU8.8.

Additionally, this report recommends extending the scope of the authority of the Chief Information Security Officer to mitigate cyber security risks across all City agencies and corporations.

In 2020, City Council established the Office of the Chief Information Security Officer, an independent cyber security division based on the Auditor General's recommendation. Initially established with just five staff members, the division has since expanded significantly to meet the growing need for cyber expertise with a team of 84 cyber security experts approved 2024 complement to address emerging cyber threats.

The team, alongside four directors, is organized into distinct business sections, each with unique functions and responsibilities, and work horizontally to provide comprehensive support. The senior management team, which consists of the Chief Information Security Officer, Deputy Chief Information Security Officer, and directors from each business section, play a pivotal role in crafting and executing the City's comprehensive cyber strategy.

Within four years, the Chief Information Security Officer has formulated the organizational structure, vision, mission, and strategy of the division and has implemented a robust and effective cyber program across the City's divisions. This program is based on established international cyber security standards including International Organization for Standardization (ISO), Statement on Standards for Attestation Engagement (SSAE), the International Society of Automation / the International Electrotechnical Commission (ISA/IEC), National Institute of Standards and Technology (NIST), and the Payment Card Industry Data Security Standard (PCI DSS).

Agencies and corporations have emerged as prime targets for cyber attacks. Government and public-sector organizations are likely to continue to be among the top targets of cyber criminals seeking financial gain or competitive intelligence in the coming years.[1]

Over the past 24 months, Toronto Zoo, Toronto Library, and Toronto Transit Commission have each experienced debilitating cyber attacks, resulting in significant disruptions to essential services provided to residents. In February 2024, the City of Hamilton suffered from a widespread and significant cyber attack which has compromised several aspects of key technology and critical infrastructure. Most recently, on March 10, 2024, the Town of Huntsville was also hit by a cyber attack, making this the second cyber attack on a municipality within a period of only three weeks.

The impact of these disruptions highlights the importance of implementing robust and effective cyber security measures to safeguard against future threats and ensure uninterrupted delivery of services to residents.

Recent cyber incidents have highlighted the vulnerability of various agencies and corporations, particularly amidst the growing trend of threat actors targeting public organizations. In light of these incidents, there is a pressing need for agencies and corporations to leverage the capabilities offered by the Chief Information Security Officer to reinforce cyber security defences and controls and be better prepared against potential breaches.

Currently, the Chief Information Security Officer's authority with respect to agencies and corporations derives from two Council Items: 2019.AU4.1 and 2021.AU10.4. These authorities do not cover the scope required by the Chief Information Security Officer to effectively address and mitigate cyber risks in agencies and corporations.

In response to these escalating threats, this report recommends extending the role of the Chief Information Security Officer to effectively identify and mitigate cyber risks across the City's wider cyber security network through more widespread use of modern cyber security techniques and technology across all agencies and corporations.

Securing digital assets owned and directly managed by the City is just one aspect of safeguarding the City's digital realm. The City invests significant resources in thoroughly assessing the cyber security measures of all suppliers and other organizations it engages with. Likewise, City agencies and corporations contribute significantly to the City's overall cyber posture, and would benefit from additional support, oversight, direction, and expertise from the City.

Fostering an environment of partnership and collaboration between the City and its agencies and corporations will serve to bolster the City's digital defences in an ever-evolving digital world.

1 The Emerging cyber security risks facing Canada's public sector

Background Information (Committee)

(April 30, 2024) Report from the Chief Information Security Officer on Extending the Mandate of the City's Chief Information Security Officer
(https://www.toronto.ca/legdocs/mmis/2024/ex/bgrd/backgroundfile-245373.pdf)
Confidential Attachment 1