TORONTO

REPORT FOR ACTION

2024 Chief Information Security Officer's Report on Agencies and Corporations

Date: October 22, 2024
To: Executive Committee
From: Chief Information Security Officer
Wards: All

SUMMARY

City Council directed the Chief Information Security Officer in EX14.3 to extend its mandate with respect to City agencies and corporations and report on responses and compliance rates of each agency and corporation to the Executive Committee in October of each year.

This report provides information about the progress that the Chief Information Security Officer has made in operationalizing the directions of City Council in EX14.3.

RECOMMENDATIONS

The Chief Information Security Officer recommends that City Council receive this report for information.

FINANCIAL IMPACT

An estimated $1.715 million is required to support the Chief Information Security Officer's extended mandate for City agencies and corporations, for professional services costs, cloud computing costs and four staff positions in the Office of the Chief Information Security Officer.

A funding request has been included for consideration in the Office of the Chief Information Security Officer's 2025 Operating Budget Submission.

The Chief Financial Officer and Treasurer has been advised of the financial impacts associated with this program to be considered along with other priorities in future budget processes.

DECISION HISTORY

On May 22 and 23, 2024, City Council adopted item EX14.3 - Extending the Mandate of the City's Chief Information Security Officer
https://secure.toronto.ca/council/agenda-item.do?item=2024.EX14.3

COMMENTS

Council Direction

On May 22 and 23,2024, City Council directed the Chief Information Security Officer to collaborate with and assist the City's agencies and corporations to do the following:

- 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;

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

- 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; and

- align their organizational cyber security frameworks with the City's overarching cyber security objectives, the City's Digital Infrastructure Strategic Framework, and established international cyber security standards.

The foundation for the City's cyber relationship with agencies and corporations are cyber policies and standards, published by the Chief Information Security Officer which provide a consistent framework for protecting sensitive information, mitigating cyber risks, and maintaining regulatory compliance. These standards are informed by international standards, such as: 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.

The City's Confirmation Program for agencies and corporations has been incorporated into the Chief Information Security Officer's extended mandate.

Actions Taken

Since receiving City Council's direction in May 2024, the Chief Information Security Officer has made rapid progress with this initiative.

Immediately following the adoption of EX14.3, the Chief Information Security Officer briefed the Executive Cyber Risk Management Group on the extended mandate. The

Executive Cyber Risk Management Group, led by the Chief Information Security Officer or their delegate, includes the administrative heads of agencies and corporations. The goal of the Executive Cyber Risk Management Group is to provide guidance and recommendations on developing, enhancing, and implementing policies, programs, strategic planning, as well as monitoring of cyber threats and providing cyber awareness training.

To support the onboarding of agencies and corporations, and to sustain the ongoing delivery of cyber services, a dedicated relationship manager role has been established by the Chief Information Security Officer.

Generally, the program has been met with enthusiasm from the agencies and corporations, with the majority eager to leverage the offerings. The agencies and corporations have expressed a willingness to collaborate, with several agencies agreeing to adopt the full range of service offerings. Some of the cyber service offerings include cyber awareness training, vulnerability management, managed email security, and endpoint detection and response.

Strategic Approach

The Chief Information Security Officer has implemented a strategic and phased approach to operationalizing the directions in EX14.3.

Phase 1 – Initial Engagement

The Office of the Chief Information Security Officer, in consultation with Legal Services, developed and distributed an onboarding package to all agencies and corporations listed in EX14.3. This onboarding package outlines the services offered by the Chief Information Security Officer, as well as legal documentation which sets out the framework for the collaborative approach to addressing the directions in EX14.3.

The Office of the Chief Information Security Officer can provide support to agencies and corporations in four key categories:

1) Cyber Risk Assessments, Consultations, and Reviews
2) Cyber Awareness and Training
3) Confirmation Program (Cyber Maturity Assessment)
4) Cyber Threat Management

In this phase, the agencies and corporations were responsible for reviewing the onboarding package and identifying resources within their organization to support the next phase.

Phase 2 – Assessment of Required Services

The Office of the Chief Information Security Officer met individually with senior management from each agency and corporation to provide information about service offerings, discuss their needs, address any concerns related to onboarding and explain the overarching goals of the mandate and requirements of agencies and corporations as directed by Council.

The Chief Information Security Officer's cyber experts have met with technical staff from each agency and corporation to identify cyber services to be leveraged and evaluate existing solutions with a view to prioritizing the implementation of services that will target key risks quickly.

In this phase, agencies and corporations were required to provide the Chief Information Security Officer with complete visibility into their existing cyber controls, and determining if they would leverage the City's key cyber services or demonstrate they had implemented or were in the process of deploying equivalent services.

Phase 3 – Agreements Executed

All parties are required to execute the necessary legal documentation to facilitate the EX14.3 initiatives: either a Memorandum of Understanding in the case of agencies, or a Professional Services Agreement in the case of Corporations. These documents provide details about the responsibilities of each of the parties, mechanisms for escalation/dispute resolution, and crystallize the service offerings which have been selected by each agency and corporation.

Phase 4 – Implementation

The implementation of cyber services has begun across the various agencies and corporations. Several cyber services have been fully deployed across agencies and corporations and are currently operational.

In addition, the Chief Information Security Officer has or will engage the boards or leadership teams of the six largest and agencies and corporations because of the complexity of their respective IT environments. These include the Boards of: Toronto Public Library, Toronto Zoo, and the Toronto Community Housing Corporation. Engagement with leadership teams or Boards of Toronto Hydro, the Toronto Transit Commission and the Toronto Police will occur in the fall of 2024 to early 2025 based on their availability.

CONTACT

Maneesh Agnihotri
Chief Information Security Officer
(416) 392-3356
Maneesh.Agnihotri@toronto.ca

SIGNATURE

Maneesh Agnihotri

Chief Information Security Officer