REPORT FOR ACTION

WITH CONFIDENTIAL ATTACHMENT

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

Date: April 30, 2024
To: Executive Committee
From: Chief Information Security Officer
Wards: All

REASON FOR CONFIDENTIAL INFORMATION

The attachment to this report involves 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

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

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.

RECOMMENDATIONS

The Chief Information Security Officer recommends:

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), 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), 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 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.

    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 (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), and
c. the City's Digital Infrastructure Strategic Framework.

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 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 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 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 this report 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, as a Shareholder direct the corporations listed in Part 2, and request the agencies listed in Part 4 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 the recommendations in this report.

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 all confidential information contained in Confidential Attachment 1 remains confidential in their entirety.

FINANCIAL IMPACT

There is no immediate financial impact from the adoption of the recommendations in this report. However, budget submissions in later years will include cyber license subscriptions, professional services cost increases and the requirement for additional staff complement due to expanding cyber services and inflationary impacts.

The Chief Financial Officer and Treasurer has reviewed and agreed with this financial impact statement.

DECISION HISTORY

2019.AU4.1- Cyber Safety: A Robust Cybersecurity Program Needed to Mitigate Current and Emerging Threats

Agencies and corporations were requested to provide cyber security risk assessments and implementation plans to mitigate cyber risks. The Chief Technology Officer's mandate was expanded to oversee standards and policies for technology assets and services for agencies, arenas, community centers, and corporations. The Chief Technology Officer was also directed to report on a plan for a centralized model that would facilitate this mandate.

2021.AU8.8 - Information Technology Projects Implementation: Information Privacy and Cybersecurity Review of Human Resource System

Item #15: The Chief Information Security Officer was requested to report to the General Government and Licensing Committee on a transformation and implementation plan for an independent and centralized cybersecurity function.

*The role of the Chief Information Security Officer was created.

2021.AU10.4 - Auditor General's Cybersecurity Review: Toronto Fire Services Critical Systems Review

The City Manager, in consultation with the Chief Information Security Officer, was directed to develop a confirmation program to address cyber risks identified in agencies and corporations and to report on the confirmation program and instances of non-compliance.

COMMENTS

Over the past four years, the Office of the Chief Information Security Officer has grown to a full-fledged team of cyber security experts. As the team expanded, so did the division's capacity, allowing it to build its cyber service offerings to provide comprehensive protection and mitigation efforts for its stakeholders. The division has also implemented a series of critical cyber security initiatives and solutions, strengthening cyber posture and cyber resilience across the City.

Organizational Structure

- **Cyber Governance:** focuses on cyber service delivery and strategic transformation to ensure operational excellence across the division.
- **Cyber Resilience:** serves as the central hub for cyber risk assessment and advisory services.
- **Cyber Advisory:** operates at the intersection of cyber awareness, cyber strategic advisory, and vulnerability management (both information technology and operational technology).
- **Cyber Threat Management:** oversees critical aspects of cyber security, focusing on offensive security, cyber intelligence, and cyber defence as well as application security.

Cyber Services

The Office of the Chief Information Security Officer offers a catalog of cyber services that is meticulously curated and regularly updated, encompassing a comprehensive array of offerings tailored to meet the evolving needs and challenges faced by City divisions and agencies and corporations. Leveraging cutting-edge technologies and industry best practices, the cyber service catalog is designed to empower divisions, agencies and corporations with the tools, insights, and support necessary to fortify their cyber defences and safeguard critical assets against an ever-expanding array of cyber threats.

Cyber Initiatives & Solutions

The Office of the Chief Information Security Officer has achieved significant milestones in strengthening the City's cyber posture and increase its cyber maturity level by 70%. Following the adoption of City Council directives 2019.AU4.1 and 2021.AU10.4, the division has partnered extensively with the City's agencies and corporations to assess cyber security risks, address vulnerabilities and develop strategies to reduce exposure to cyber threats.

- **Cyber Risk Assessments** are conducted for new technology and/or systems and where major changes are implemented to existing technology and/or systems. In 2023, nearly 600 comprehensive cyber risk assessments were completed marking a 270% %increase compared to the previous year.

- **Cyber Culture and Awareness** initiatives are being implemented among elected officials, staff, contractors, and suppliers accessing the City's network, in addition to participating agencies and corporations. Over 28,000 hours of cyber awareness training were provided in 2023. The education of our end users has resulted in a 23% reduction in the click rate of phishing simulations compared to the same period last year, and a 55% decrease since 2021.

- **Cyber Secure Procurement** protocol was devised in consultation with the Chief Procurement Officer, the City Clerk, the City Solicitor, and the Chief Technology Officer. This protocol integrates cyber security and privacy requirements into the initial phases of the procurement process to ensure suppliers provide products and services consistent with industry best practices.

- **Amendment to Chapter 195, Purchasing Bylaw** was developed in consultation with the Chief Procurement Officer and the City Solicitor to insert a requirement for all City divisions to consult with the Technology Services Division and the Office of the Chief Information Security Officer when procuring goods or services that may have implications for the City's technology infrastructure and its cyber security posture. This amendment is scheduled to come into force on July 1, 2024.

- **Cyber-Secure Centralized Login Platform** incorporates industry best practices with a single-entry point for the public to access city online services. When fully implemented, it will eliminate multiple login platforms, improve customer experience, and enhance cyber security and privacy. The pilot launched in December 2023 to Children's Services' My Child Care Account and will be implemented across additional city online services.

CONTACT

Andree Noel
Deputy Chief Information Security Officer

SIGNATURE

Maneesh Agnihotri
Chief Information Security Officer

ATTACHMENTS

Confidential Attachment 1