TORONTO

REPORT FOR ACTION WITH CONFIDENTIAL ATTACHMENT

Outstanding Cybersecurity Recommendations from Auditor General Reports – Chief Information Security Officer Status

Date: June 22, 2021
To: Audit Committee
From: Interim 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.

SUMMARY

The Auditor General reviews the implementation status of recommendations made through her audit and investigation reports. The results of the review are reported to City Council through the Audit Committee.

The Auditor General has conducted a number of audits since 2015 to assess cybersecurity controls of the City's IT infrastructure, systems, and applications. As per the Auditor General's latest report, there are 43 recommendations related to cybersecurity that have not been fully implemented. The Office of the CISO currently has access to 28 of those recommendations through the audit tracking tool, TeamMate.

At its meeting on April 7 and 8, 2021, City Council adopted Item AU8.5, Auditor General's Follow-Up of the Outstanding Recommendations - Status Update, without amendments and without debate.
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2021.AU8.5

At its February 16, 2021 meeting, the Audit Committee recommended that:

> "City Council request the Chief Information Security Officer to report to the May 31, 2021 meeting of the Audit Committee on the implementation status of all outstanding cybersecurity-related audit recommendations, including:

a. high priority recommendations where there are still significant risks;

b. risks being faced by the City of Toronto as a result of not implementing audit recommendations;

c. a risk assessment identifying the impact of the risks after considering any current vulnerabilities;

d. any other security risks being faced as a result of the changing cyber threat landscape; and

e. short-, medium-, and long-term plans identifying what needs to be done to reduce the risk level for the City of Toronto in an expedited fashion."

The Office of the CISO has conducted an assessment based on the above criteria and this report provides an update on the status of high priority outstanding recommendations. As the May 31, 2021 Audit Committee meeting was cancelled, this report is being tabled for the July 7, 2021 Audit Committee meeting.

This report pertains to the 28 high priority cybersecurity recommendations currently accessible to the Office of the CISO in TeamMate. The Office of the CISO will continue its assessment of the remaining recommendations, including an assessment of additional security risks related to the changing cyber threat landscape. The Office of the CISO will report on these additional recommendations at the next Audit Committee meeting.

The Office of the CISO (OC) has assessed the residual risk of the high priority recommendations based on remediation progress and compensating controls in the current environment. In summary, 3 of the recommendations have been fully implemented. Additionally, the OC has determined that 21 of the 28 recommendations remain on track to be implemented within 2021 (short and medium terms). The assessment has identified 13 high risk recommendations plus 3 additional risks the City faces due to the continuously changing cyber threat landscape. Due to the recent global attacks on the critical infrastructure, it's therefore extremely important that the implementation of these recommendations be expedited.

Table 1 below captures the status of all 28 recommendations* as shown in TeamMate and their associated risk ratings based on the risk assessment (*as of June 22, 2021):

Category	High Risk	Medium Risk	Low Risk	Total
Cyber Risk Program	3	1	2	6
Policies and Standards		4	1	5
Threat Management	5	1		6
Technical Standards	4	1	1	6
Awareness and Training			2	2
Fully Remediated	1		2	3
TOTAL	13	7	8	28

Table 2 below highlights the associated remediation timeline for open recommendations:

Remediation Timeline	High Risk	Medium Risk	Low Risk	Total
Short Term (September 30, 2021)	6	3	4	13
Medium Term (December 31, 2021)	5	1	2	8
Long Term (September 30, 2022)	1	3		4
TOTAL	12	7	6	25*

* 3 recommendations are fully implemented.

Other Major Risks (in addition to open recommendations)

The ever-evolving cyber threat landscape can create new and unexpected challenges for the City. Social engineering, ransomware and increased use of third party software are some other major cybersecurity risks that could impact the City's critical infrastructure in the near future.

Management Actions

The following actions are underway in partnership with the Technology Services Division (TSD) to reduce the cyber risk exposure at the City:

Short Term – On boarded cybersecurity vendor partner and MSSP (managed security services provider), in partnership with TSD, to help standardize cybersecurity policies, procedures, tools and threat management practices across the City.

Medium Term – Implementing cybersecurity controls along with logging and monitoring tools across all City divisions (IT infrastructure, systems and applications).

Long Term – Achieve long term cyber maturity tied back to ISO 27001/NIST Frameworks, implement Threat Risk Assessments (TRA) and Cyber Risk Assessments (CRA) on an ongoing basis. Additionally, the City should continue to work on projects such as Microsoft 365, Privileged Access Management (PAM) and Cloud Security implementation to limit the risks emerging from access controls, third party software and cloud computing.

RECOMMENDATIONS

The Interim Chief Information Security Officer recommends that:

1. City Council direct that Confidential Attachment 1 remain confidential in its entirety, as it involves the security of property belonging to the City of Toronto.

FINANCIAL IMPACT

There are no financial impacts as a result of the recommendation in this report.

Any costs associated with implementing these recommendations are accommodated within the 2021 Operating Budget for the Office of the Chief Information Security Officer.

DECISION HISTORY

The follow-up of outstanding recommendations is required by Government Auditing Standards. The process is important as it ensures that management has taken appropriate actions to implement the recommendations from previous audit reports. The follow-up review is part of the Auditor General's Annual Work Plan. The Auditor General reports to the Board of Directors and the City's Audit Committee each year on the implementation status of outstanding recommendations.

Due to the importance of the cybersecurity recommendations, and as a result of the February 16, 2021 Audit Committee request, the Office of the Chief Information Security Officer was directed to separately report on the status of the high risk recommendations. City Council adopted this recommendation at its meeting on April 7 and 8, 2021 without amendments and without debate.
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2021.AU8.5

COMMENTS

The Office of the CISO is thankful to the City Clerk, the City Manager's Office, the Technology Services Division, Toronto Water and the Auditor General's Office for their support in the delivery of this report.

The remediation of cyber risks requires the establishment and implementation of an end-to-end Cybersecurity program. While significant efforts have been undertaken by City divisions in improving the cyber risk awareness since 2019, the implementation of some of these recommendations were delayed last year due to the onset of COVID-19. In 2020, the Office of the CISO, in partnership with TSD, on boarded a managed security service provider and is working with its vendor partners for the implementation of a Cybersecurity program for the City. Due to the City's massive IT infrastructure, implementation of this program requires extensive partnerships and support from multiple stakeholders. The Office of the CISO will continue to work with all City Divisions to ensure these high priority cybersecurity risks are actioned within the revised timelines.

Definitions of other major risks:
1. Social Engineering – range from phishing attacks where victims are tricked into providing confidential information, vishing attacks where an urgent and official sounding voice mail convinces victims to act quickly or suffer severe consequences.

2. Ransomware – is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. With the recent attack on major pipeline in US, ransomware has emerged as a major threat to critical infrastructure.

Canadian Security Magazine recently published an opinion on some recent attacks on critical infrastructure:

OPINION: Cyber-attacks can shut down critical infrastructure. It's time to make cyber security compulsory - Canadian Security Magazine

3. Third Party Software – Occurs when someone infiltrates City's system through an outside partner or provider with access to City's systems and data. Supply chain vulnerabilities have led to some of the most dramatic cyber-attacks in recent years. The recent SolarWinds attack which impacted almost 18,000 customers globally is an example of risks posed by third parties (vendors and software). The City was not impacted by this attack.

Harvard Business Review recently reported on the vulnerabilities that arise due to third-party software emphasizing that "Leaders need new ways to reduce supply chain cybersecurity risks, whether they're buying digital products or producing them".

Is Third-Party Software Leaving You Vulnerable to Cyberattacks? (hbr.org)

Background on the Office of the CISO:

In 2019, the Chief Information Security Officer position was created. The first CISO for the City of Toronto was hired in October, 2019. The office of the CISO (OC) was established as an independent division in January 2020. Currently the OC has six (6) business units supporting all City divisions:

Cyber Diplomacy and Governance - Implement proactive cyber strategies, programs, policies and strategic initiatives. Provide Cyber Risk advisory services to support the fulfillment of City's strategic objectives.

Business Application Resilience - Enable the delivery of secure business applications through the development and implementation of secure system development lifecycle (security by design).

Digital Forensics and Investigations - Digital forensics and investigations related to misconduct. Collaborates with law enforcement and government.

Digital Trust - Provide a safe, convenient and seamless way to access the City's digital government services. Foundation to verify who we are online, while protecting our personal information.

Threat Management - Provide services to identify and respond to, internal and external cyber threats affecting the City of Toronto. Provide strategic and tactical guidance in response to cyber breaches.

Urban Technology Protection - Responsible for the protection of underlying technology running the Critical Infrastructure of the City (impact on life safety, democracy, citizens).

CONTACT

Abiodun Morolari, Interim Chief Information Security Officer, 416-396-4693,
Abiodun.Morolari@toronto.ca

SIGNATURE

Abiodun Morolari
Interim Chief Information Security Officer

ATTACHMENTS

Confidential Attachment 1