TORONTO

REPORT FOR ACTION

Establishment of the City's Cyber Security Program to Enable Vulnerability Assessment and Penetration Testing

Date: June 20, 2019
To: Audit Committee
From: Chief Information Officer
Wards: All

SUMMARY

This report responds to Audit Committee's request to report on the Information and Technology Division's outstanding audit recommendation wherein the Chief Information Officer was requested to develop a Cyber Security Program that supported ongoing vulnerability assessment and penetration testing using industry standards applied by subject matter experts.

The City already has a foundation of cyber security measures in place to protect the City's information technology systems. The Auditor General's recommendations will enhance existing cyber security practices and assist with the detection, prevention and responses to future cyber threats. The City launched its formal Cyber Security Program in 2017 to enhance security capabilities given the increasing complexity in cyber security. The objective of this Program is to identify and mitigate IT-related risks that directly affect the corporate technology environment that City Divisions rely upon when servicing the residents and the public who expect the provision of secure and reliable City services.

One component of the Cyber Security Program includes the analysis of resources and funding requirements to develop and implement improvements to vulnerability assessments and penetration testing functions. In addition, the City plans to implement new vulnerability management capabilities as part of a strategy to engage a Managed Security Services Provider (MSSP) and develop partnerships with industry experts.

Further to the above recommendation, the Chief Information Officer, in collaboration with the Auditor General's Office, will be issuing a comprehensive Audit Report to Audit Committee for its meeting on October 25, 2019. This report will provide a comprehensive review of all audit recommendations (including both public and confidential) received to date.

RECOMMENDATIONS

The Chief Information Officer recommends that:

1. Audit Committee receive this report for information.

FINANCIAL IMPACT

This report has no net financial impact on the City of Toronto.

The Chief Financial Officer and Treasurer have reviewed this report and agree with the financial impact information.

DECISION HISTORY

At its meeting on March 31, 2016, City Council adopted item AU5.10, Audit of Information Technology Vulnerability and Penetration Testing - Phase 1: External Penetration Testing, providing the results of the external vulnerability assessment and penetration testing of internet facing applications used by the public.
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2016.AU5.10

At its meeting on May 3, 2019, Audit Committee adopted item AU2.6, Auditor General's Response to the Audit Committee's Request on the Outstanding Audit Recommendations Which Are of Greatest Concern, requesting the appropriate City staff to report to the Audit Committee at its meeting on June 28, 2019, on the following outstanding recommendations identified by the Auditor General in Attachment 1 to the report dated April 16, 2019:
• Facilities Management, Audit of City Cleaning Services Recommendations 3 and 9;
• Information and Technology Recommendation 2; and,
• Pension, Payroll and Employee Benefits Recommendations 3, 7 and 15.
http://app.toronto.ca/tmmis/viewAgendaItemHistory.do?item=2019.AU2.6

COMMENTS

The ability to manage cyber threats is considered one of the most critical operational risks facing public organizations. As cyber security's importance continues to grow, government networks and systems remain under threat due to hacking and other forms of cyber-attacks. These security breaches of information technology systems can have a profound impact on both the City and its residents.

In 2016, the Auditor General recommended to City Council that the Chief Information Officer develop a Cyber Security Program that includes ongoing vulnerability assessment and penetration testing using current tools used by industry subject matter experts. Further, the Auditor General identified that any testing tools adopted by the City should be updated regularly and provide ongoing reporting and metrics around existing and newly discovered threats. At its meeting on May 3, 2019, Audit Committee requested that the Chief Information Officer report back on this recommendation.

The Information and Technology Division established a formal Cyber Security Program in 2017. As a result of this program, Information and Technology staff have a better understanding of the cyber security risks the City is facing and have taken steps to implement appropriate cyber security practices.

The Cyber Security Program has three core streams of activity:

1. Cyber Security Maturity Assessment: The City hired an external consultant to assess the City's current cyber security posture independently. The assessment reviewed the maturity level of the City's enterprise security capabilities against the generally-accepted industry best practice frameworks and compared our practices to other cities worldwide to identify and prioritize where enhancements should be made. The assessment will conclude in July 2019.

2. Managed Security Services: A Request for Proposal was issued on May 15, 2019 and is closing on July 3, 2019 to procure a Managed Security Services Provider. The goal of the procurement is to acquire services to supplement existing security practices in the City to proactively detect, prevent and mitigate threats and support response to incidents. The results of this procurement initiative will be reported to the General Government and Licensing Committee.

3. Cyber Security Awareness and Training: The goal of this program is to educate all city staff on how to recognize and report possible cyber threats, and how to safely use the City's IT infrastructure and assets. Phase 1 of the program launched in Q4 2018 with cyber security awareness communication activities across the City and further formal City-wide Cyber Security Awareness Training will begin this summer with further phases to follow.

In addition to the above-noted activities, I&T Division continues to deliver on-going vulnerability assessment, penetration testing and threat risk assessment services to internal project teams to identify and manage cyber risks and has security tools in place to mitigate risk on the IT Infrastructure.

Further to the above recommendation, the Chief Information Officer, in collaboration with the Auditor General's Office, will be bringing forward a comprehensive report forward to Audit Committee for its meeting on October 25, 2019. This report will provide a complete review of all outstanding audit recommendations for all audits applicable to the I&T Division.

CONTACT

Grant Coffey, Director, Strategy and Program Management, Information and Technology Division
Tel.: 416-392-9759, Email: Grant.Coffey@toronto.ca

SIGNATURE

Rob Meikle
Chief Information Officer