AUDITOR GENERAL'S REPORT
ACTION REQUIRED
with Confidential Attachment

Audit of Information Technology Vulnerability and Penetration Testing – Phase 1: External Penetration Testing

Date:	February 16, 2016
To:	Audit Committee
From:	Auditor General
Wards:	All
Reason for Confidential Information:	This report involves the security of property belonging to the City or one of its agencies and corporations.
Reference Number:	

SUMMARY

Insufficient preparation to manage cyber threats is widely considered one of the most critical operational risks facing organizations today. According to KPMG, "*Cyber security has become an enormous issue in the last few years and its importance continues to grow. Major corporations' networks and systems continue to be subject to hacking and attack*", and it "*is therefore essential for Audit Committees to understand what management is doing to mitigate IT risks.*"

Security breaches of information technology (IT) systems can have profound effects on organizations. The confidentiality, integrity and availability of IT systems is essential for the operations of the City. It is important that the City maintains the public's trust that its websites and the City's data are secure.

The Auditor General's 2015 Audit Work Plan included an audit of information technology network vulnerabilities within the City. This report provides the results of the external vulnerability assessment and penetration testing of internet facing applications used by the public. A separate assessment of controls over the internal IT network of the City will be completed later in 2016.

This report contains two recommendations along with management's response to each recommendation. Additionally, a confidential report with confidential recommendations and management's response to each recommendation is included in Attachment 1.

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council request the Chief Information Officer to establish the City baseline for cybersecurity applicable to all of the City's IT systems and infrastructure and to direct all City divisions, agencies, and corporations to adhere to this standard. The Chief Information Officer establish protocols for monitoring and enforcing compliance with this City-wide standard.

2. City Council request that the Chief Information Officer to develop a cybersecurity program that includes ongoing vulnerability assessment and penetration testing using current tools used by industry subject matter experts. The testing tools adopted by the City should be updated regularly and provide ongoing reporting and metrics around existing and newly discovered threats.

3. City Council adopt the Confidential Recommendations contained in Confidential Attachment 1 to the report (February 16, 2016) from the Auditor General.

4. City Council direct that Confidential Attachment 1 remain confidential in its entirety as it contains confidential information involving the security of property belonging to the City or one of its agencies and corporations.

Financial Impact

The implementation of the recommendations in this report will strengthen information technology controls. The extent of costs and/or resources needed to implement the recommendations is not determinable at this time. However, the cost of improved controls to manage and respond to cyber threats are counterbalanced against the potentially significant costs that would result from security breaches, such as, data clean-up, statutory fines and litigation.

Historically the Auditor General's Office has undertaken limited IT security audits. To receive proper assurance about the security of IT systems, the Auditor General needs additional resources. The Auditor General's 2016 operating budget request included a request for $50,000 to continue with her IT audits. At this time, this budget has not been approved.

ISSUE BACKGROUND

The Auditor General's 2015 Audit Work Plan included an audit of information technology network vulnerabilities within the City.

The purpose of this audit is to assess whether the City's information technology systems and assets are adequately protected from external and internal threats. This audit is being performed in two phases:

- Phase I focuses on the external vulnerability assessment and penetration testing of internet facing applications used by the public.

- Phase II includes a detailed assessment of controls over the internal IT network of the City. Vulnerability assessment and penetration testing from inside the City will be performed during the second phase of the audit.

This report provides the results of the first phase of our audit. The results for Phase II, the audit of the City's internal IT network, will be issued later in 2016.

Auditing IT vulnerabilities is a highly specialized area. This audit required the combined information technology skills of audit staff and the expertise of external consultants. The external vulnerability assessment and penetration testing, performed by an external consultant under the direction and supervision of the Auditor General's Office, was designed to simulate the approach and techniques that a skilled attacker would use to find weaknesses in the City's IT systems.

The audit methodology included the following:

- Meetings with the external consultant and the corporate Information & Technology Division to define the scope of testing, emergency contacts and notification protocols
- Identification of in-scope applications, testing scenarios, risks and testing exclusions
- Performing the vulnerability assessment, scanning and analysis using specialized tools to execute automated and/or manual security testing
- Investigation and validation of findings

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

COMMENTS

The confidentiality, integrity and availability of information technology systems is essential for the operations of the City. It is extremely important that the City maintains the public's trust that its websites and the City's data are secure. Any breach of the City's systems could cause operational issues and delays and may result in significant financial exposures including loss of revenue to the City.

A single corporate view of cyber security is needed

The City of Toronto has a complex network consisting of over 25,000 computers, servers and other hardware equipment, over 700 business applications, three data centres and several City facilities connected to serve the citizens of Toronto.

While the corporate Information & Technology Division acts as a City-wide coordination point, the management of the City's IT infrastructure and business applications is not fully centralized. Responsibility is distributed amongst:

- The corporate Information & Technology Division
- The City Clerk's Office that provides IT and technology planning support for the City Clerk's Office and Offices of the Mayor, Councillors, and Accountability Officers
- Divisional information technology staff who support business applications

Consequently, there is no single corporate view of cyber security. The decentralized approach to information technology systems and security results in differing perspectives, risk tolerances, and levels of maturity when identifying and responding to cyber risks.

A unified City-wide approach to managing cyber threats is needed. The City's Chief Information Officer should establish the City baseline for cybersecurity applicable to all of the City's IT systems and infrastructure, regardless of which division, agency or corporation is responsible for managing business applications.

The U.S. based National Institute of Standards and Technology has developed a Cybersecurity Framework. This Framework is based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risks. The City could use the Framework as a guide that could be customised to address, for example:

- The City's current cybersecurity posture
- The City's target state for cybersecurity
- Opportunities for improvement that should be identified and prioritized within the context of a continuous and repeatable process
- Assessment of progress towards the target state
- Communication among internal and external stakeholders about cybersecurity risks.

All divisions, agencies, or corporations responsible for managing any specific aspect of the City's IT infrastructure and business applications should be expected to adhere to this framework.

Recommendation 1:

City Council request the Chief Information Officer to establish the City baseline for cybersecurity applicable to all of the City's IT systems and infrastructure and to direct all City divisions, agencies, and corporations to adhere to this standard. The Chief Information Officer establish protocols for monitoring and enforcing compliance with this City-wide standard.

Vulnerability assessments and penetration testing should be performed for all City systems

Vulnerability assessment is the practice of testing and evaluating the security of IT systems and applications to find vulnerabilities that an unauthorized attacker could exploit. An attacker (hacker) is characterized as someone who identifies one or more of the weaknesses that exist within an IT system and penetrates them to gain access to obtain confidential and sensitive information and for any other malicious intent.

Not all City IT systems are included in an ongoing program of vulnerability assessments and/or penetration testing. To ensure effective safeguards are in place to ensure the confidentiality, integrity and availability of IT systems and applications, vulnerability assessments and penetration tests are strongly recommended. Vulnerability assessments and penetration testing should be used to verify the strength of controls applied to the City's IT systems.

Recommendation 2:

City Council request the Chief Information Officer to develop and implement a cybersecurity program that includes ongoing vulnerability assessments and penetration testing using current tools used by industry subject matter experts. The testing tools adopted by the City should be updated regularly and provide ongoing reporting and metrics around existing and newly discovered threats.

Management's response to the two recommendations contained in this report is attached as Appendix 1. Additionally, a confidential report with confidential recommendations and management's response to each recommendation is included in Attachment 1.

Finally, we would like to express our sincere thanks to the Risk Management & Information Security, Technology Infrastructure Services, and Enterprise Solutions Delivery teams from the corporate Information & Technology Division, as well as, City Clerk's IT personnel for their efforts in providing cyber security to the City, and for their cooperation and support during the audit.

CONTACT

Ina Chan, Assistant Auditor General, Auditor General's Office
Tel: 416-392-8472, Fax: 416-392-3754, E-mail: ichan3@toronto.ca

Syed Ali, Audit Director, IT & Strategy, Auditor General's Office
Tel: 416-392-8438, Fax: 416-392-3754, E-mail: sali4@toronto.ca

SIGNATURE

____

Beverly Romeo-Beehler, Auditor General

ATTACHMENTS

Attachment 1 – Confidential Information:
Audit of Information Technology Vulnerability and Penetration Testing – Phase I: External Penetration Testing

Appendix 1: Management's Response to the Auditor General's Audit of Information Technology Vulnerability and Penetration Testing – Phase I: External Penetration Testing

APPENDIX 1

Management's Response to the Auditor General's
Audit of Information Technology Vulnerability and Penetration Testing – Phase I: External Penetration Testing

Rec No.	Recommendations	Agree (X)	Disagree (X)	Management Comments: *(Comments are required only for recommendations where there is disagreement.)*	Action Plan/Time Frame
1.	**City Council request the Chief Information Officer to establish the City baseline for cybersecurity applicable to all of the City's IT systems and infrastructure and to direct all City divisions, agencies, and corporations to adhere to this standard. The Chief Information Officer establish protocols for monitoring and enforcing compliance with this City-wide standard.**	X			The CIO will direct appropriate individuals within the I&T Division to develop a baseline for cybersecurity, as well as protocols for monitoring and enforcing compliance, targeted to be in place by Q4 2017. The resulting baseline and associated protocols will be published and made available for other divisions, agencies, and corporations by Q1 2018. The CIO will issue a memo compelling the divisions, agencies, and corporations to become compliant with the published standards. The CIO will make Risk Management, Cyber Security and Compliance resources available to assist in evaluating compliance.
2.	**City Council request the Chief Information Officer to develop and implement a cybersecurity program that includes ongoing vulnerability assessments and penetration testing using current tools used by industry subject matter experts. The testing tools adopted by the City should be updated regularly and provide ongoing reporting and metrics around existing and newly discovered threats.**	X			The CIO will direct the appropriate Corporate I&T resources to undertake an analysis of the resources and funding required to develop and implement a vulnerability management and penetration testing function, as part of the overall cybersecurity program that comprises industry best practices, tools, methodologies. The analysis will be completed by Q3 2016, and program implementation will be completed by Q1 2017.