TORONTO

AUDITOR GENERAL'S REPORT
with Confidential Attachment

Audit of Information Technology Vulnerability and Penetration Testing – Phase II: Internal Penetration Testing, Part 1 – Accessibility of Network and Servers

Date:	October 24, 2016
To:	Audit Committee
From:	Auditor General
Wards:	All
Reason for Confidential Information:	**Reasons for confidentiality** This report involves the security of property belonging to the City or one of its agencies and corporations.
Reference Number:	

SUMMARY

In early 2016, the Auditor General completed the external vulnerability assessment and penetration testing of the City's information technology (IT) network. The external testing involved vulnerability assessment and penetration testing of the City systems, applications and infrastructure from externally exposed links, such as, websites and servers. The goal was getting from outside to inside.

This Phase II, Part 1 report relates to the internal testing of the City's IT network, servers and systems. This included targets similar to external testing, but from within the organization, i.e., the tester has some limited access to the City facilities, network and applications. The goal was to identify vulnerabilities that can be exploited from inside the City to gain access to City systems and infrastructure for malicious intent. The Auditor General has decided to present the results early to enable management to take timely action.

Phase II testing is divided into two parts:

- Part 1 – Accessibility of Network and Servers
- Part 2 - Application Vulnerability Assessment and Penetration Testing

The existing segmented approach for ownership of IT security and administration has resulted in varied policies, procedures and enforcement of security practices across the City. Similar to the findings reported in the Phase I audit, the results of Phase II, Part 1 – Accessibility of Network and Servers reinforces the need to have a single corporate view of IT security within the City. KPMG, in their report entitled *Cyber security: it's not just about technology*[1], notes that "*Effectively managing cyber security risk means putting in place the right governance and the right supporting processes, along with the right enabling technology*".

Divisions that have independent IT units that acquire systems and implement applications present the risk of having security practices that may not align with Corporate IT standards and may also not have required security expertise. It is important for Corporate IT to be accountable for managing City-wide information security.

The details of our findings are provided in the confidential attachment to this report. The Auditor General will retest the vulnerabilities identified after the implementation of the recommendations to ensure that the issues identified in this report have been appropriately remediated by management.

RECOMMENDATIONS

The Auditor General recommends that:

1. City Council adopt the Confidential Recommendations contained in Confidential Attachment 1 to the report (October 24, 2016) from the Auditor General.

2. City Council direct that Confidential Attachment 1 to the report (October 24, 2016) 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 findings have been discussed with management to allow for timely corrective action. At this point, the financial impact, if any, is not determinable.

ISSUE BACKGROUND

Auditing IT vulnerabilities is a highly specialized area. The audit team consisted of audit staff and the expertise of external consultants. The internal vulnerability assessment and penetration testing was designed to simulate the approach and techniques that an attacker

[1] Cyber security: it's not just about technology
https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-security-not-just-technology.pdf

would use to find and exploit weaknesses in the City's IT systems. The testing was performed on a sample of IT systems, network and servers.

In one of its publications, the US Department of Homeland Security defines an insider threat as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misuses that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems.

The same publication references a recent study that notes local area network (LAN) access as the top target area for insider threats and misuse, followed by physical threats and remote access vulnerabilities.

While Part 1 of the Phase II review provides in general terms the current state of IT security, a more descriptive and technical report will be provided to management upon completion of this audit. The Auditor General will update the Audit Committee and Council accordingly.

Our Phase 1 report on external vulnerability assessment and penetration testing is available at:
http://www.toronto.ca/legdocs/mmis/2016/au/bgrd/backgroundfile-90751.pdf

COMMENTS

The confidentiality, integrity and availability of information technology systems are essential for City operations. Any breach of City systems could cause operational and service interruptions which may result in significant financial exposure, including loss of public trust and integrity of data.

The audit methodology included the following:

- Meetings between the external consultant and Corporate Information & Technology Division staff 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 with IT management.

A confidential report with confidential recommendations and management's response to each recommendation is included in the Confidential Attachment 1.

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.

CONTACT

Julian Lebowitz, Audit Manager, Auditor General's Office
Tel: 416-392-8473, Fax: 416-392-3754, E-mail: jlebowi@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

ATTACHMENT

Attachment 1 – Confidential Information:
Audit of Information Technology Vulnerability and Penetration Testing – Phase II: Internal Penetration Testing, Part 1 – Accessibility of Network and Servers