City of Markham

Cyber Security Audit

Auditor General's Report

PREPARED BY: MNP LLP
300 - 111 Richmond Street West
Toronto, ON M5H 2G4

MNP CONTACT: Geoff Rodrigues, CPA, CA, CIA, CRMA, ORMP
Partner, National Internal Audit Leader
PHONE: 416-515-3800
FAX: 416-596-7894
EMAIL: geoff.rodrigues@mnp.ca

March 26, 2018

March 26, 2018

Mayor and Members of Council,

I am pleased to present the cyber security audit report ("report") of the Auditor General for the City of Markham (the "City").

The results of the audit are representative of the security controls as of September 15, 2017. Our report was discussed with the management and executive leadership team.

This report is provided to you for information and consideration, as you review and approve the City's proposed action plans.

Sincerely,

Geoff Rodrigues, CPA, CA, CIA, CRMA, ORMP

Auditor General, City of Markham

TABLE OF CONTENTS

STATEMENT OF LIMITATIONS

The Auditor General's work was limited to specific procedures and analysis. We planned and performed our audit to assess whether the controls were reasonable to meet the applicable security standards. Changes in circumstances after the report date could affect the findings. The projection to the future of any evaluation of the controls to achieve the related control objectives is subject to the risk that controls may become inadequate or fail. Selecting and relying on a specific portion of the analysis or factors considered by MNP in isolation may be misleading.

BACKGROUND

Many organizations, including municipalities like the City of Markham ("City"), find it challenging to protect against today's cyber security threats and cyber adversaries, who are often financially motivated and find value in a range of information, from sensitive contracts, intellectual property, to financial and personal records. Attacks can originate from many different sources, including organized hacking groups, internal staff, and disgruntled former employees, to name a few. Further, the avenue of attacks continues to evolve, as we see attackers shift their efforts from hacking into external facing systems, to attacks that directly target personnel through targeted malware and social engineering. These types of attacks effectively bypass traditional defenses like perimeter firewalls and anti-malware software.

While we see an increasing trend of "yet another security breach" being reported, perhaps what is more troubling to consider is the fact that many more breaches may not be disclosed at all. There is generally no incentive for an organization to report a security breach because of the potential financial and reputational impact, so until mandatory breach requirements are in place, we may only be seeing the tip of the iceberg. Many organizations may not even be aware that a security breach has already occurred. The Verizon 2017 Data Breach Investigations Report describes public sector organizations as having the third highest number of reported breaches, not far behind the financial and healthcare industries.

In addition to valuable information stored on traditional corporate systems, there are emerging risks as attackers target industrial control systems that could have significant impact to the City. As these systems converge with corporate IT systems and become more interconnected, the expanded impact to the exposed attack surface needs to be considered. While the City does not have a large number of industrial control systems, it does manage a water pumping station control system that if an attacker were to target, may cause significant disruption and harm to the citizens of Markham.

A comprehensive security program is required to mitigate these threats and without one there is an increased risk of an information security incident or data breach which may have a significant and negative impact on the City. An effective and comprehensive security program forms the foundation for the implementation of security practices and it comprises a structured and tailored plan to manage these security risks. Furthermore, it needs to be continually monitored and maintained, to address the requirements of business, as well as the changing security threat landscape.

In our role as the Auditor General for the City, MNP LLP ("MNP") performed procedures to evaluate the effectiveness of the City's IT security controls, including policies, procedures and IT security governance activities.

This report contains a summary of our observations and recommendations, along with management's response. A confidential report with detailed observations has been provided to management as a separate attachment.

OBSERVATIONS

Recognizing the security threats to its IT systems, the City has made efforts to reduce their exposure to cyber security risks and protect its IT systems and data. We noted elements that demonstrate the City's continued commitment to protecting its key IT systems and information, including protective measures in important control areas around perimeter network defenses, anti-malware protection, encryption, IT system backups, administrative access, vulnerability assessments, and security of mobile devices.

Notwithstanding the security practices in place, we noted that the City has not formally and sufficiently defined a comprehensive security program, that is sustained with a supporting security strategy and

roadmap, security policies, and dedicated resources who are responsible for monitoring and maintaining the City's security posture. Maintaining an effective security program requires ongoing effort, provides the structure and foundation to manage security risks, and evolves with business requirements as well as the changing security threat landscape.

There is no one-size-fits-all approach and each organization should formally define their program based on risk appetite and leveraging industry accepted frameworks. Taking a formal and comprehensive approach to address the detailed observations discussed in the confidential report will strengthen the City's security posture. The financial cost and resources needed to implement the recommendations will need to be assessed and prioritized, taking into consideration aspects such as management's tolerance for security risk, as well as the potentially significant costs and reputational impact that would result in the event of a security breach.

RECOMMENDATIONS

The Auditor General recommends that:

1. The Cyber Security Audit – Auditor General's Report be received;

2. The City be directed to enhance the City's current security program by formalizing efforts and priority for cyber security. The City should determine the level of security that they wish to achieve, improve their existing practices, and monitor progress towards its security objectives; and,

3. City staff be authorized and directed to do all things necessary to give effect to these recommendations.

MANAGEMENT'S RESPONSE

Management supports the recommendations made by the Auditor General. The City will enhance its current cyber security practices by developing a comprehensive security program that will include:

- Security strategy and roadmap;
- Security policies and procedures;
- Identification of budget and resources required; and,
- Targeted priorities and dates to address the gaps identified in the confidential report.

The security program will provide a sustainable approach to enhance the City's cyber security posture based on the level of risk tolerance deemed appropriate by the City.

The program will be developed by external resources with expertise in this area.

Timeline: The draft program will be completed by **Q3 2018** for senior management approval and decision making.