CITY OF VAUGHAN

EXTRACT FROM COUNCIL MEETING MINUTES OF DECEMBER 15, 2015

Item 1, Report No. 17, of the Finance, Administration and Audit Committee, which was adopted without amendment by the Council of the City of Vaughan on December 15, 2015.

1 INTERNAL AUDIT REPORT – AUDIT OF INFORMATION TECHNOLOGY SECURITY CONTROLS

The Finance, Administration and Audit Committee recommends:

1) That the recommendation contained in the following report of the Director of Internal Audit, dated December 8, 2015, be approved;

2) That the presentation by the Director of Internal Audit and C2, presentation material titled "*Audit of Information Technology Security Controls*" dated December 8, 2015, be received; and

3) That the deputation by Mr. Richard Lorello, Treelawn Boulevard, Kleinburg, be received.

Recommendation

The Director of Internal Audit recommends:

1. That the Internal Audit Report on the Audit of Information Technology Security Controls be received.

Contribution to Sustainability

Internal Audit activities and reports contribute to the sustainability of the City by providing advice and assurance that controls supporting the effective delivery of services and programs are effective. Longer term sustainability needs the support of good, efficient risk mitigation strategies. Internal Audit can provide support for that sustainability by providing independent advice and assurance.

Economic Impact

There are no direct economic impacts associated with this report.

Communications Plan

Not applicable.

Purpose

To present to the Finance, Administration and Audit Committee the Internal Audit Report on the Audit of Information Technology Security Controls.

Background - Analysis and Options

Securing computerized data and information is important for a number of reasons, but principally as a means of keeping information safe. The importance of computer security lies in how harmful it can be if data or information is lost.

The City stores a lot of data, some of it very sensitive, including payment information, staff records, e-mails, citizen information and extensive corporate documents, both finished and those in progress.

In addition to security breaches by outsiders, there is also an increasing risk that data and systems can be compromised by staff inside organizations. As part of their daily responsibilities, staff have access to data and information that those outside of the organization typically do not. Although not a risk unique to computerized information, the ease of availability and accessibility to computerized information significantly increases the likelihood of a security breach.

Relationship to Term of Council Service Excellence Strategy Map (2014-2018)

This report supports the Term of Council Priority: Continue to Advance a Culture of Excellence in Governance, and the Service Excellence Initiative: Improvement Through Technology.

Regional Implications

Not applicable.

Conclusion

Computerized data security is in an evolutionary phase at the City of Vaughan. A recent third party review of the City's critical security controls indicated that the City compares favorably to other municipalities that had a similar review done. However, the review did identify improvements that would further strengthen controls. Improving security is an ongoing activity that needs to be well planned based on risk and cost. The Information and Technology Management Department (ITM) is currently engaged in this process.

The City has good processes to help detect and prevent malicious attacks, has secure configuration standards for new computers and has good reliable backup data.

Of the recommended improvements, there are some that would reduce risk without major financial, procedural or technical changes to the computing environment. These improvements or "quick wins" include better device and software management that would help lower the risk of unauthorized or unmanaged hardware and software being present on the network and using a vulnerability scanning tool or service to monitor potential attacks on the system network.

Although having foolproof security in place is not a realistic goal, it would be prudent for the City to maximize the "quick wins" to improve security while keeping costs and disruption low. ITM has recognized this and is risk assessing its priorities to maximize security improvements.

Attachment

1. Internal Audit Report – Audit of Information Technology Security Controls

Report prepared by:

Paul Wallis CPA, CMA CIA CISA CRMA
Director, Internal Audit

(A copy of the attachments referred to in the foregoing have been forwarded to each Member of Council and a copy thereof is also on file in the office of the City Clerk.)

INTERNAL AUDIT REPORT –
AUDIT OF INFORMATION TECHNOLOGY SECURITY CONTROLS

Recommendation

The Director of Internal Audit recommends:

1. That the Internal Audit Report on the Audit of Information Technology Security Controls be received.

Contribution to Sustainability

Internal Audit activities and reports contribute to the sustainability of the City by providing advice and assurance that controls supporting the effective delivery of services and programs are effective. Longer term sustainability needs the support of good, efficient risk mitigation strategies. Internal Audit can provide support for that sustainability by providing independent advice and assurance.

Economic Impact

There are no direct economic impacts associated with this report.

Communications Plan

Not applicable.

Purpose

To present to the Finance, Administration and Audit Committee the Internal Audit Report on the Audit of Information Technology Security Controls.

Background - Analysis and Options

Securing computerized data and information is important for a number of reasons, but principally as a means of keeping information safe. The importance of computer security lies in how harmful it can be if data or information is lost.

The City stores a lot of data, some of it very sensitive, including payment information, staff records, e-mails, citizen information and extensive corporate documents, both finished and those in progress.

In addition to security breaches by outsiders, there is also an increasing risk that data and systems can be compromised by staff inside organizations. As part of their daily responsibilities, staff have access to data and information that those outside of the organization typically do not. Although not a risk unique to computerized information, the ease of availability and accessibility to computerized information significantly increases the likelihood of a security breach.

Relationship to Term of Council Service Excellence Strategy Map (2014-2018)

This report supports the Term of Council Priority: Continue to Advance a Culture of Excellence in Governance, and the Service Excellence Initiative: Improvement Through Technology.

Regional Implications

Not applicable.

Conclusion

Computerized data security is in an evolutionary phase at the City of Vaughan. A recent third party review of the City's critical security controls indicated that the City compares favorably to other municipalities that had a similar review done. However, the review did identify improvements that would further strengthen controls. Improving security is an ongoing activity that needs to be well planned based on risk and cost. The Information and Technology Management Department (ITM) is currently engaged in this process.

The City has good processes to help detect and prevent malicious attacks, has secure configuration standards for new computers and has good reliable backup data.

Of the recommended improvements, there are some that would reduce risk without major financial, procedural or technical changes to the computing environment. These improvements or "quick wins" include better device and software management that would help lower the risk of unauthorized or unmanaged hardware and software being present on the network and using a vulnerability scanning tool or service to monitor potential attacks on the system network.

Although having foolproof security in place is not a realistic goal, it would be prudent for the City to maximize the "quick wins" to improve security while keeping costs and disruption low. ITM has recognized this and is risk assessing its priorities to maximize security improvements.

Attachment

1. Internal Audit Report – Audit of Information Technology Security Controls

Report prepared by:

Paul Wallis CPA, CMA CIA CISA CRMA
Director, Internal Audit

Respectfully submitted,

Paul Wallis CPA, CMA CIA CISA CRMA
Director, Internal Audit

Attachment 1

VAUGHAN

INTERNAL AUDIT REPORT

Audit of Information Technology Security Controls

September 2015

CONCLUSION AND SUMMARY

Computerized data security is in an evolutionary phase at the City of Vaughan. A recent third party review of the City's critical security controls indicated that the City compares favourably to other municipalities that had a similar review done. However, the review did identify improvements that would further strengthen controls. Improving security is an ongoing activity that needs to be well planned based on risk and cost. The Information and Technology Management Department (ITM) is currently engaged in this process.

The review indicated that good processes are in place to:

- help detect and prevent malicious attacks to City networks and data
- ensure secure configuration standards are used and implemented when new computer assets are added to the City
- ensure that reliable backup data is available should the need arise.

Of the recommended improvements, three would reduce risk without major financial, procedural or technical changes to the computing environment.

These include:

- managing all hardware devices on the network so that only authorized devices are given access and unauthorized and unmanaged devices are found and prevented from gaining access
- managing all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation and execution
- using a vulnerability scanning tool or service to monitor potential attacks on the system network.

Although having foolproof security in place is not a realistic goal, it would be prudent for the City to maximize the "quick wins" to improve security while keeping costs and disruption low. ITM has recognized this and is risk assessing it priorities to maximize security improvements.

The City has a Municipal Security Policy but it is 30 years old. A more up-to-date "Terms of Use for City of Vaughan Computing and Telecommunications Facilities" document is signed by all new staff and is displayed daily when staff log in to the City's computing facilities. This document provides conditions for using the computing facilities but it is not a fully developed corporate security policy. ITM is currently working on an Information Technology Security Policy which is more directed towards ITM management and staff. Work on a fully developed up-to-date user or staff Security Policy is expected to begin later as the City's security program evolves.

ITM has one staff responsible for developing a security program. Currently, the focus is on identifying critical systems and risk assessing priorities. Work has also begun on developing a Security Office IT Operations Manual. This manual will contain the guidelines, procedures and standards needed to support the computer security environment for the City.

Depending on available resources and ITM priorities, it is expected that all major components of the program including policies, standards and procedures will be in place by the end of 2016.

We will follow up on the status of outstanding Management Action Plans related to this audit and will report the status to the Finance, Administration and Audit Committee.

BACKGROUND

Securing computerized data and information is important for a number of reasons, but perhaps principally as a means of keeping information safe. The data and related information that most organizations and users store on their hard drives are often far more valuable than the machines themselves. Broadly speaking, the importance of computer security lies in how harmful it can be if that data or information is lost.

The City stores a lot of data, some of it very sensitive, including payment information, staff records, e-mails, citizen information and extensive corporate documents, both finished and those in progress.

Computers are not inherently open to risks such as hacking or data breach. In order for outsiders to get into a computer, that computer must somehow open itself up to intrusion. Internet activity is the primary highway for these transactions. Simply accessing the web makes computers more vulnerable.

There is also an increasing risk that data and systems can be compromised by staff inside organizations. Staff has access to data and information that those outside of the organization typically do not. Although not a risk unique to computerized information, the ease of availability and accessibility to computerized information significantly increases the likelihood of a security breach.

OBJECTIVES AND SCOPE

The objective of the audit was to evaluate the adequacy and effectiveness of the internal controls, processes and procedures in place to mitigate the business risks related to securing computerized information and data on City networks and computers.

Although all staff at the City have a responsibility for securing computerized data and information, the scope of this review was focused on ITM. ITM has responsibility for setting policy, developing standards and for providing awareness and education to staff on computer security.

ITM had a third party service provider evaluate the Critical Security Controls maturity for the City. This review focused on measuring security and providing metrics on both the strong and weak areas of computer security.

The review also provided advice on a prioritized method for planning security approaches to rapidly improve security.

Internal Audit reviewed the approach the third party used and decided to rely on the testing done to support the audit. A brief description of the approach used to evaluate computer security at the City is in the attached Appendix on Page 9.

Auditors: Paul Wallis CMA, CPA CIA CISA CRMA

Author: Paul Wallis CMA, CPA CIA CISA CRMA

Director: Paul Wallis CPA, CMA CIA CISA CRMA

DETAILED REPORT

1. *Critical Security Controls Maturity Assessment*

In June 2015, the Information and Technology Management Department [ITM] engaged the services of a third party vendor to do a Critical Security Control review for the City of Vaughan. The Critical Security Controls [CSC] are twenty prioritized, well vetted, and supported security controls that organizations can use to assess and improve security. The CSC is a set of recommended actions for cyber defense that provide specific and actionable ways to stop today's most pervasive attacks. They were developed and are maintained by a consortium of hundreds of security experts from across the public and private sectors. An underlying theme of the Controls is support for large-scale, standards-based security automation for the management of cyber defenses. The CSC process can also be seen as a “foundational risk assessment” that can be used as a starting point for immediate, high value action. While there a number of information security standards that identify more controls, the CSC is often seen as the quickest way to focus first on prioritizing security functions that are effective against the latest advanced targeted threats.

Based on the vendor’s review, the City has security strength in the following areas:

- **Malware Defenses** - Malicious or harmful software can be a dangerous aspect of Internet threats. The malicious software can attack systems, services and data. In addition, modern malware can be designed to avoid defenses, or to attack and disable them.

  ITM has good tools in place to help detect and prevent malicious attacks.

- **Securing Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers –** Manufacturers’ default configurations for operating systems and applications are usually set up for ease of use rather than good security. Attackers look for and take advantage of weak passwords, default accounts and other open targets.

  ITM has good processes in place to ensure secure configuration standards are used and implemented when new computer assets are added to the City.

- **Data Recovery Capability –** When computerized devices are compromised, there is the possibility that changes can be made to data potentially impacting organizational effectiveness with polluted information.

  ITM has reasonable processes in place to ensure that reliable backup data is available should the need arise.

The third party vendor had a number of other recommendations to further improve security. The intent of ITM is to eventually address the key areas but in a way that is based on a balance of priorities, cost and overall risk to the City.

A component of the CSC model is the identification of “quick wins”. These are described as opportunities to significantly reduce risk without major financial, procedural or technical changes to the computing environment. The model further identifies the “First Five Quick Wins” that enable a highly focused application of controls that have the most impact on preventing attacks.

Of the five, the third party vendor recommended the following as a priority to further develop security maturity.

- **Inventory of Authorized and Unauthorized Devices** – Manage all hardware devices on the network so that only authorized devices are given access and unauthorized and unmanaged devices are found and prevented from gaining access. This reduces the risk of unauthorized access to City resources through untested or compromised devices.

- **Inventory of Authorized and Unauthorized Software** – Manage all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation and execution. This reduces the risk of unauthorized software from infiltrating the network leading to the potential alteration or corruption of data and services.

- **Continuous Vulnerability Assessment and Remediation** – Keep up-to-date on emerging vulnerabilities and make changes to the computer network to reduce the opportunity for new threats. This reduces the risk of attackers taking advantage of new vulnerabilities to access systems that were previously secure.

Management Action Plan

To address “Inventory of Authorized and Unauthorized Devices” critical security control ITM is planning to launch two projects “Asset Inventory Discovery” and “Network Access Control”, estimated to be fully deployed by Q1 2017. Main deliverables will be an electronic asset discovery tool and deployment of technology preventing unauthorized access to corporate network and resources.

To address “Inventory of Authorized and Unauthorized Software” critical security control ITM is planning to launch two additional projects “Unauthorized Software Control” and “Software Standards for Client and Server Systems”. Main deliverables will be pre-approved software list and a tool to enforce software standards on IT infrastructure. “Software Standards for Client and Server Systems” is estimated to be delivered by Q4 2016. Software package required for implementation of “Unauthorized Software Control” will be selected and implementation cost estimates would be compiled by Q4 2016 with the intention to fully deploy the system by the end of 2017, if necessary budget is approved.

To address “Continuous Vulnerability Assessment and Remediation” critical security control ITM has launched an operational initiative led by IT Security Officer, on July 6, 2015, to evaluate industry leading vulnerability scanning offerings. The goal is to procure necessary tools and configure scanning of critical infrastructure. The tool will be used to help identify and prioritize remediation measures as well as concentrate resources on the most significant vulnerabilities. Scheduled for completion by Q1 2016.

2. *Data Protection [Security] Policy*

The purpose of a data security policy is to outline the roles and responsibilities for creating and maintaining an environment that safeguards data from threats to personal, professional and City interest. A policy is also designed to establish processes for protecting confidential information and to establish administrative, technical and physical safeguards to protect against unauthorized access or use of information.

The protection and dissemination of information and the related data at the City is governed by the Municipal Freedom of Information and Protection of Privacy Act [MFIPPA]. The legislation generally outlines what needs to be protected and what can be publicly disclosed but does not cover how it should be done.

Computerized data is not just restricted to ITM servers and other devices. With the proliferation of mobile devices such as USB drives, smartphones, tablets and other devices containing personal data, the risk of accidental loss and disclosure are magnified.

The City has a Municipal Computer Security policy that outlines that computers are to be used for municipal business only and that municipal computer system security is the responsibility of ITM. Setting procedures and monitoring personal computers remains with department heads and individual staff members. This policy, however, has not been updated since 1986.

The City also has a “Terms of Use for City of Vaughan Computing and Telecommunications Facilities” document that is signed by all new staff and displayed daily prior to system login. Although not a security policy, it does provide general conditions staff must accept prior to using City computing facilities. This document was last updated in 2010.

Even though all management and staff do have a responsibility, it should be more clearly outlined in an up-to-date policy with guidance to support appropriate accountability and responsibility.

Management Action Plan

In 2015, ITM department has launched an operational initiative to develop a new, comprehensive security policy geared towards IT department personnel. It is scheduled to be completed by Q3 2016. A set of supplemental acceptable use policies geared towards general user community and covering the use of Remote Access, Wi-Fi, Laptops, Tablets, Other Mobile Devices, Removable Electronics Media, E-mail and Internet is scheduled to be completed by Q4 2016. ITM department is collaborating with established IT security experts as well as consulting various industry standards and best practices to ensure quality and relevance.

3. *Security Program*

The purpose of a system security program is to provide an overview of the security requirements of the City's systems and describe the controls in place or planned for meeting those requirements. A system security program also outlines the responsibilities and expected behavior of all individuals who access the system. The program, including the relevant standards and guidelines, should be viewed as documentation for supporting the planning of adequate, cost-effective security protection.

The program should reflect input from various managers with responsibilities concerning the system, including information and system owners.

The risk of not having a fully documented program is that data and system security roles and responsibilities could become unclear. The absence of standards could lead to an overall program that, in turn, could be costly yet not protect the riskier City data and system assets. This could result in exposures leading to non-compliance with legislation and damage to the City's reputation.

The City of Vaughan does not have a fully documented security program. ITM has begun work on developing a Security Office IT Operations Manual. The framework of the Manual is based on meeting various globally recognized data and information security standards.

Work on this will take time as risks specific to the City have to be identified and the investment in tools will have to be recognized in future budgets.

We support the development of a security program and feel it is a significant step in reducing the risks associated with unauthorized data access and disclosure.

Management Action Plan

ITM department has launched various initiatives in 2014-2015 to establish and formalize the following major components of IT security program:

- **Vulnerability Scanning**
- **IT Infrastructure Penetration Testing**
- **Risk Assessment and Remediation**
- **IT Security Incident Response**
- **IT Security Key Performance Indicators**
- **Security Awareness Training**

All components would be fully documented and integrated into ITM operations by Q4 2016.

APPENDIX

Critical Security Controls for Effective Cyber Defense

Over the years, many security standards and requirements frameworks have been developed in attempts to address risks to enterprise systems and the critical data in them. However, most of these efforts have essentially become exercises in reporting on compliance and have actually diverted security program resources from the constantly evolving attacks that must be addressed. In 2008, this was recognized as a serious problem by the U.S. National Security Agency (NSA), and they began an effort that took an "offense must inform defense" approach to prioritizing a list of the controls that would have the greatest impact in improving risk posture against real-world threats. A consortium of U.S. and international agencies quickly grew, and was joined by experts from private industry and around the globe. Ultimately, recommendations for what became the Critical Security Controls were coordinated through the SANS Institute, a computer security training, certification and research organization. In 2013, the stewardship and sustainment of the Controls were transferred to the Council on CyberSecurity, an independent global non-profit entity committed to a secure and open Internet.

The Critical Security Controls focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works" - security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness.

Standardization and automation is another top priority, to gain operational efficiencies while also improving effectiveness. The Controls prioritize and focus on a smaller number of actionable controls with high-payoff, aiming for a "must do first" philosophy. Since the Controls were derived from the most common attack patterns and were vetted across a very broad community of government and industry, with very strong consensus on the resulting set of controls, they serve as the basis for immediate high-value action.