COMMITTEE OF THE WHOLE (WORKING SESSION) NOVEMBER 27, 2007

SYSTEMS INTEGRITY REVIEW

Recommendation

The Chief Information Officer (CIO) in consultation with the Deputy City Manager / Commissioner of Finance & Corporate Services and the Director of Information Technology & Telecommunications recommends:

1. That this report be received for information, and
2. That the presentation by the Chief Information Officer (CIO) be received, and
3. That the presentation by Legend Corporation be received, and
4. That Council confirms that staff are to proceed with item #18 contained in the Systems Integrity Review Recommendations (Attachment 1), and
5. That item #19 contained in the Systems Integrity Review Recommendations (Attachment 1) be referred to the Budget Committee.

Economic Impact

The overall assessment of the City's Information Technology (IT) Security framework is that it is effective and compares well with other organizations with similar security requirements as the City. A number of further improvements to the overall security framework were proposed and are in the process of being implemented. Most of these improvements are focused on internal procedures and controls and sufficient funding is available in previously approved budgets.

One initiative that will require additional funding is the implementation of a structured journaling and archiving technology solution for the corporate eMail system (item #19 contained in the Systems Integrity Review Recommendations – Attachment 1). It is estimated that this solution may cost in the range of $60,000 to $160,000. A Capital Budget request has been submitted for consideration by the Senior Management Team and the Budget Committee for this initiative.

Communications Plan

n/a

Purpose

The purpose of this report is to provide Council with an executive summary of a recent comprehensive Information Technology (IT) systems integrity review and the resulting undertakings to further enhance overall computing environment security.

Background - Analysis and Options

The City's Information and Technology Management (ITM) department conducts regular assessments of corporate computing environment security. Such assessments are intended to identify potential weaknesses in the overall computing environment security framework, assess risk levels of identified weaknesses, and to implement appropriate remedies to mitigate significant risk.

Typically, security assessments are focused on single specific elements of the City's computing environment security framework, such as applications security, network security, device security, etc. During the Summer of 2007, a comprehensive IT integrity review was carried out which focused on multiple critical elements of the IT infrastructure, including internal procedures and controls.

System Integrity Review Methodology

The objective of this IT systems integrity review was to identify opportunities to enhance the overall IT security framework in order to increase protection of data and to improve auditing capabilities for data access. To accomplish this objective, current internal processes, procedures and controls were compared to IT industry best practices for systems security. To ensure objectivity and enable access to the most comprehensive IT industry benchmarks for security, the ITM department engaged the services of external IT security experts.

Legend Corporation is a Microsoft Gold Certified partner, and an IT industry award-winning expert in security solutions. Under the leadership of Legend Corporation, the following elements of the City's corporate IT computing environment were assessed and benchmarked:

- eMail Security Controls
- eMail Audit Trailing practices
- Enterprise Security Policy Management (Active Directory Services)
- Administrative Procedures and Controls
- Data Recovery Procedures and Controls
- Biometric Identification Technologies
- eMail Encryption
- Information Rights Management

Bell Security Solutions Team is a division of Bell Canada Enterprises and a recognized IT industry expert in network security. Under the leadership of Bell Security Solutions Team, the following elements of the City's corporate IT computing environment were assessed and benchmarked:

- Firewall Devices Configuration and Management
- Network Architecture and Perimeter Review
- Vulnerability Testing Against Hacking Attacks from the Internet

Both Legend Corporation and Bell Security Solutions Team used proven auditing methods for their respective assessments and benchmarking. The audit methodology included:

- Interviews with key IT personnel
- Acquisition and review of existing configuration documentation
- Acquisition and review of existing procedural documentation
- Interactive observation and review of network systems and resources
- Acquisition and analysis of data through the use of tools and utilities
- Testing and validation of established controls

In addition to the security assessments performed by external experts, ITM staff have also reviewed internal procedures surrounding the administration and use of BlackBerry devices and eMail journaling and archiving solutions. Internal staff findings and recommendations are reflected in the IT systems integrity review findings section below.

IT System Integrity Review Findings

The respective comprehensive IT system integrity reviews carried out by Legend Corporation and Bell Security Solutions Team concluded that the overall City of Vaughan IT security framework compared well to the IT industry best practices. The City's overall IT security framework is effective and meets the City's functional and business requirements. In some areas of the City's IT security framework, the controls exceed other companies of similar size and risk tolerance.

During the course of the review, opportunities to improve system integrity based on the City's current internal practices compared to IT industry best practices were observed. These were classified as minor in nature and do not pose significant security risk. ITM staff has acknowledged all observations in the external experts' reports and have undertaken to implement appropriate remedies to further enhance the City's overall IT security framework.

The primary recommendations and their status are listed in Attachment 1. In Attachment 1 there are a total of 19 recommendations, with the exception of #18 and #19, staff are proceeding to implement the changes. Recommendation #18 relates to the encryption of members of Council messages. The presentation will include comments regarding encryption and staff are requesting confirmation if Council wishes to proceed. Item #19 requires funding and is recommended be referred to the 2008 budget process for consideration.

Relationship to Vaughan Vision 2007

This report is consistent with the priorities previously set by Council and the necessary resources to undertake the review have been allocated and approved. Additional resources will be required to fully implement the recommendations. Specifically, the recommendations of this report support the following City strategic objectives:

A1 – Pursue Excellence in Service Delivery
C1 – Demonstrate Leadership and Promote Effective Governance
C2 – Enhance Productivity, Cost Effectiveness and Innovations

Regional Implications

n/a

Conclusion

The comprehensive IT integrity review that was carried out by Legend Corporation and Bell Security Solutions Team concluded that the overall City of Vaughan IT security framework compared well to the IT industry best practices. The City's overall IT security framework is effective and meets the City's functional and business requirements. In some areas of the City's IT security framework, the controls exceed other companies of similar size and risk tolerance.

During the course of the audit, opportunities to improve system integrity based on the City's current internal practices compared to IT industry best practices were observed. These were classified as minor in nature and do not pose significant security risk. ITM staff have acknowledged all observations in external experts' reports and have undertaken to implement appropriate remedies to further enhance the City's overall IT security framework.

Attachments

ATTACHMENT 1 – Systems Integrity Review – Recommendations

Report prepared by:

Dimitri Yampolsky, Chief Information Officer (CIO) – 8352
Jack Dhaliwal, Director of Information Technology & Telecommunications – 8132

Respectfully submitted,

Dimitri YAMPOLSKY
Chief Information Officer

Jack DHALIWAL
Director of Information Technology & Telecommunications

ATTACHMENT 1 – SYSTEMS INTEGRITY REVIEW – RECOMMENDATIONS

	Recommendations and Undertakings	Status / Comments
1.	Reduce the number of systems administrators and segregate specific administrative functions	IMPLEMENTED
2.	Establish a formal approval process for Administrators actions	IMPLEMENTED
3.	Implement logging of Administrators actions	IMPLEMENTED
4.	Change current administrators procedures to require data owner approval / consent for data management functions	IMPLEMENTED
5.	Implement a formal requisition procedure and approval controls for data recovery and access	IMPLEMENTED
6.	Implement "Group Policies" to enforce password, screen saver, and event logging rules	In Progress TBC in 30 days
7.	Update anti-virus product to recent version on 5 of the 50 servers	In Progress TBC in 90 days
8.	Increase the frequency of security updates (to guard against virus and hacking vulnerabilities) from quarterly to monthly cycle on back-end servers, including Exchange servers and Active Directory servers	In Progress TBC in 90 days
9.	Establish criteria for use of encryption technologies and make available to implement as appropriate to enhance data access controls	In Progress
10.	Establish criteria for use of enterprise biometric technology solutions and implement where appropriate to enhance device and network access controls	In Progress
11.	Establish criteria for use of information rights management technologies and implement where appropriate to enhance data confidentiality controls	In Progress
12.	Consider using an off-site facility, such as the Joint Operations Centre for disaster recovery purposes	In Progress TBC in 2008
13.	More detailed documentation of current policies, practices and procedures to provide formal governance for Firewall security	In Progress TBC in 90 days
14.	Documentation of operating procedures for Firewalls	In Progress TBC in 90 days
15.	Process changes to Firewall security through existing formal Change Control process	IMPLEMENTED
16.	Maintain a log of Firewall security changes	IMPLEMENTED
17.	BlackBerry User Procedures for device security	In Progress TBC in 90 days
18.	Provide members of Council with eMail encryption certificates to enable encryption of messages, and provide appropriate training to members of Council	Requires Confirmation
19.	Implement a formal and structured eMail journaling and archival system in order to discontinue the current practice of saving eMail archives on users' personal computers	Requires Budget Approval $60K - $160K TBC in 2008

Notes: TBC = To Be Completed