TORONTO STAFF REPORT

February 27, 2001

To: Audit Committee

From: City Auditor

Subject: Windows NT Security Review

Purpose:

To report on the review of the security standards and practices followed in administering the Windows NT environment.

Financial Implications and Impact Statement:

There are no direct financial impacts arising from this report.

Recommendation:

It is recommended that this report be received for information.

Background:

Included in Audit Services 2001 work plan is a project entitled, "Network Server Security Profiles". The primary objective of this project is to ensure that the administration and security practices, which govern the City's network environments, are commensurate with identified risks. We have completed this review for the Windows NT network environments administered within Corporate Services, Works and Emergency Services and Toronto Public Health.

Detailed reports have been issued to the relevant Commissioners for Corporate Services and Works and Emergency Services departments. Due to the sensitivity of the information with regard to the City's security practices these reports have been distributed as private and confidential. Observations for Toronto Public Health have been reported to management within the responsible organization unit. Since the most significant finding relates to physical security and is addressed in the report to the Commissioner for Corporate Services a separate report relating to the Public Health Division is not warranted. Further reports will be issued as additional components of the City's network environment are reviewed.

The Windows NT Server Operating Systems, controlled by the Information and Technology Division of the Corporate Services Department and to a lesser extent divisions within other departments, is the backbone supporting access to computing resources for the majority of the City's employees. Uninterrupted service and the highest level of security for this network is critical in ensuring that City staff can continue to perform their day to day duties.

The City's network users are divided into various departmental and divisional clusters. These clusters are known as domains. The logical grouping of users in these domains is useful in controlling the access of groups of users to data and resources. The Windows NT Server Operating System provides the ability to link or join two or more domains into a single administrative unit. This allows each user to have a single logon account regardless of the number of domains they need to access. At December 31, 2000, the corporate domain, under the administration of the Information and Technology Division, consisted of 12,000 Windows NT workstations with approximately 14,000 users. Sixteen departmental domains are linked to the corporate domain. These 16 departmental domains, plus several other domains used for controlling local resources are administered within departments.

Rather than examine all 16 of the departmental domains, we selected a sample of the Windows NT servers for review. Our sample selection was designed to cover a large number of users while at the same time selecting from different departmental clusters to allow for identification of differences in the implementation of security features and administrative procedures.

Comments:

The Information & Technology Division have, for the most part, driven the evolution of the structure of the City's Windows NT network environment, also known as the network architecture. There has been little or no corporate direction guiding the development of the current architecture or related security policies and procedures. The architecture is being shaped as a result of continuous negotiation between the Information & Technology personnel and department personnel.

The Information Technology Division has taken the lead in establishing a corporate domain and drafting a Windows NT Server Standards & Administration document. However, the value and effectiveness of this effort is limited in the absence of support at the corporate level and a vehicle to implement and enforce the standards across the entire City. The results of the Windows NT Security review reinforces the need for the City to institute a more formal approach to dealing with practices, procedures and technology solutions that cross organizational boundaries.

The review indicated corporate-wide policies, standards or guidelines available to the Windows NT administrators responsible for maintaining the Windows NT servers, although in existence, had not been communicated. This is a contributing factor for the inconsistent application of the available security features provided by the Windows NT operating system. Requiring compliance with corporate standards represents an opportunity to improve the overall level of security in the Windows NT operating system.

Physical security over the servers used to administer domains at the department level was found to be inadequate. A plan to relocate as many of these servers as possible to the secure environment of the corporate data centre is an issue that requires consideration. Although there may be certain servers which departments may not want to move to the data centre, these should be the exception and a business case should be made for servers remaining in the department.

Finally, the City has a software tool that permits the Information & Technology Division to independently monitor and control resources, both hardware and software, that are connected to the corporate domain. Resources not attached to the corporate domain can not be tracked using this tool. Further consolidation of individual domains into the corporate domain will enhance the City's ability to control the organization's Information and Technology assets.

Conclusions:

Management responsible for those Windows NT domains examined as part of this review have initiated corrective action to address many of the concerns included in the detailed reports we have issued. However, the ability to implement and enforce policies and standards associated with technology on a corporate wide basis is critical to ensure that the concerns identified as a result of this review, are addressed across the entire organization. We have discussed the need for a corporate presence in the provision and control of information and technology services in a report dated February 26, 2001, entitled "Information Security Framework". Implementation of the recommendations of that report will assist in providing the necessary environment to support consistent security practices and solutions across the entire corporation.

Contact:

Jerry Shaubel, Director, Audit Services, Tel: (416) 392-8462, Fax: (416) 392-3754
E-Mail: JShaubel@city.toronto.on.ca

Jeffrey Griffiths
City Auditor

dl

C:\DATA\audit\2001\Reports\Corporate Services\I & T\Windows NT Audit Report - Feb 27.doc