Office of the Auditor General

AUDIT OF INTERNET USAGE AND CONTROLS

2005 REPORT

Chapter 8

Table of Contents

Executive Summary

1.1 Introduction

The Audit of Internet Usage and Controls was part of the 2005 audit plan brought forward by the City's Auditor General and received by City Council on December 15, 2004.

1.2 Background

There are approximately 9,000 users of the Internet within the City of Ottawa. All users have access to e-mail, World Wide Web, and other Internet communications protocols (for example, MSN messenger chat, FTP, and specialized library catalogue systems protocols) within the City of Ottawa. To facilitate this communication and transfer of information, the City has 220 high-speed wide-area network connections and 60 dial-up connections.

Information Technology Services Branch reported a total of 26.7 million Internet "hits", performed by 6,226 users who accessed the Internet during the month of October 2005, which represents an average of 4,282 hits per user for that month.

The City's e-mail systems transfer over 200,000 e-mails daily.

The use of the City's Internet and e-mail services are regulated and governed through two (2) policies. For the purpose of this audit, we reviewed the following policies, which were in effect at the time of our review:

- Responsible Computing Policy (August 13, 2001); and
- Responsible Use of the Internet Policy (December 11, 2003).

The Ottawa Public Library (OPL) has a requirement for increased flexibility and less restrictive filtering of Internet and e-mail content that result in less stringent application of security controls.

1.3 Audit Scope

The audit scope is limited to Information Technology (IT) strategy, policies, procedures and other controls (including the technical tools) that define and control the City of Ottawa's use of the Internet. In particular, the following were reviewed:

- Information Management/Information Technology (IM/IT) Security strategy
- Responsible Use policies
- Incident investigation policies
- Service request policies
- Firewalls
- Anti-Spam filtering
- Anti-Virus filtering
- Content filtering
- 8 large City sites and 6 small City sites
- Internet traffic (sites visited) for conformance to Responsible Use of the Internet Policy
- E-mail usage for compliance to policy

The Ottawa Police Service was not included in the audit.

1.4 Audit Objective

The audit objective is to provide an independent and objective assessment of:

- The adequacy, effectiveness and reliability of security strategy, policy, measures and controls in place over the usage of the Internet and e-mail; and
- To determine whether Internet and e-mail usage is compliant with City policies.

1.5 Key Findings and Recommendations

The key findings and recommendations from this audit can be summarized in the following items.

On the whole, the e-mail controls to safeguard system/information confidentiality, integrity and availability worked as expected. Specifically, we found that the security controls surrounding the e-mail isolation of dangerous attachments were successful. Even though knowledgeable users were found to be able to bypass file type blocking controls, they were not able to bypass anti-virus controls and the nine anti-virus engines blocked malicious file content.

Although, we found that Library and Employment Centre Public Desktop Lockdown could be greatly improved from providing an automated Windows XP patching, and the latest Symantec Antivirus version.

Finally, we determined that the implementation of the anti-spam firewall in January 2004 had greatly reduced the amount of SPAM e-mail that City staff must process and, reduced the possibility of the SPAM setting off a malicious software infestation, and reduced the e-mail delivery system resource requirements.

Recommendation 1

That Information Technology Services investigate the tools used to perform blocking by file type to enable this feature regardless of extension.

Recommendation 2

That Information Technology Services deploy the latest Symantec Antivirus version.

Recommendation 3

That Information Technology Services update the configuration of the Antivirus systems to include anti-virus checking on read from disk and before program execution.

Management Response

Management agrees with recommendations 1, 2 and 3.

IT Services is investigating a new feature recently available for the first layer of virus-scanning protection, which permits blocking of file types regardless of the extension used. Testing to ensure there is no negative impact on e-mail delivery services will occur in Q1 2006.

IT Services considers that the risk of using the current version of Symantec Antivirus (7.61) is mitigated as three additional layers of anti-virus and malicious file protection also safeguard the City network, and Symantec continues to issue updated virus signature files per the support agreement up to January 31, 2006.

It is not uncommon for an organization of the size of the City of Ottawa to delay or skip version upgrades of software products. Upgrades are done either because the new functionality offered is needed by the City and is supported by a business case for the upgrade, or because the product is no longer supported by the vendor. IT Services has evaluated the additional features and business case for each new version as it is released. In fact, the City partnered with Symantec in Q1 2005 to beta-test version 10, as this is the first version to add features to safeguard against the current threat from spyware. Following this evaluation, Symantec recommended in late Q3 2005 that the City begin a managed upgrade directly from version 7.61 to Symantec Antivirus version 10.

IT Services initiated the upgrade to Symantec Antivirus 10 in Q4 2005, to be completed by January 31, 2006. This upgrade includes an assessment of the productivity impact of including anti-virus checking on read from disk and before program execution.

Recommendation 4

That Information Technology Services:

- **Review the level of awareness of the SPAM e-mailbox and increase visibility if warranted; and**
- **Continue monitoring of the effectiveness of the current SPAM filtering tool.**

Management Response

Management agrees with these recommendations.

The spam@ottawa.ca mailbox continues to be part of IT Services' ongoing security awareness program. Over 1,000 e-mails received by City staff from external sources are submitted monthly to the SPAM mailbox for review. In addition, four City Brief articles were published in 2005 on the topic of SPAM, each including a reminder about the availability of the SPAM mailbox. IT Services will continue to remind staff of the SPAM e-mailbox regularly.

Upgrades to the SPAM filtering service are implemented by IT Services when available from the vendor, to ensure continued effectiveness of the service. As noted in the report, monitoring of the SPAM filtering service is performed daily, and reviewed monthly by IT Services.

October data from MessageLabs indicated that 65% of all e-mail worldwide was identified as SPAM. Of the 50,000 e-mails received from external sources daily to the City's 9,000 e-mail users, slightly over 50% is identified as SPAM and immediately rejected. Roughly 0.5% of these e-mails are SPAM that is not identified or rejected, and successfully reaches a City recipient – 250 e-mails per day for the entire City. Users are encouraged to forward SPAM messages to IT Services to assist in increasing the effectiveness of the SPAM filtering service.

HTTP Web Site Filtering

While the Websense content filtering tool is generally regarded as a success, it also identifies a key weakness to the overall City security posture. The City network is a homogenous group of devices without separation from one another by security controls. The implication is that an outbreak of a security incident can quickly impact all systems on the network. The City security model relies on strong perimeter security to help prevent such incidents. Most users on the City network are protected through a variety of protective security devices largely associated with the perimeter. The Ottawa Public Library users are partially exempt from some of these controls. The result is that the strong perimeter security controls are negated potentially allowing malicious code to move onto the City network. This bypass of some controls is a weakness in the security posture of the City.

Recommendation 5

That Information Technology Services:

- **Tighten the Websense service implementation to reduce possibility of service bypass.**

  Management Response

  Management agrees with this recommendation.

  In 2005, prior to the audit, IT Services launched an extensive project to enhance the rigour of the Websense implementation, scheduled for completion in Q1 2006. At the time of writing this response (November 2005), an extensive range of additional Websense filtering features is now in place.

  The audit findings identified one small site (the Don Gamble Community Centre) that allowed City of Ottawa staff unfiltered access to the Internet. This was a subnet routing issue that misidentified these four City staff to Websense as Library staff workstations, which are unfiltered (see below). IT Services has corrected this routing issue.

- **Review some level of Library filtering to reduce the risk, such as a limited number of isolated general use systems for unfiltered web access. If this cannot be completed to an appropriate level, then Information Technology Services should consider separating the Ottawa Public Library from the City's system.**

  Management Response

  Unfiltered Internet access is provided to Ottawa Public Library (OPL) staff for reasons of intellectual freedom. This is as a result of a Library Board directive and therefore is a governance issue with the Library Board and outside the jurisdiction of the IT Services Branch.

  Since 2001, a considerable amount of effort from IT Services has been directed to manage the risk of this configuration. For example, Library workstations are on separate network segments that make it easy to isolate viruses, worms and spyware in the event of a malicious code outbreak. On the advice of IT Services staff, Library Management agreed, in October 2005, to allow IT Services to protect their workstations from Internet-borne malicious code. The workstations used by Library staff do not allow staff to visit malicious websites, however they remain completely unfiltered for all other website content.

Given the OPL is governed by the Library Board, it may not be possible to influence the Board to reverse the decision to allow unlimited access to Internet sites based on the principle of intellectual freedom. Therefore if filtering cannot be implemented to a reasonable level, ITS Branch agrees with the recommendation that consideration should be given to separate the Ottawa Public Library from the City's system. This would be a significant undertaking as the Ottawa Public Library (OPL) is spread across 33 different sites throughout the City. Furthermore, separating the Ottawa Public Library from the City of Ottawa network would incur significant additional costs, due to the sharing of business applications and IT Services resources between OPL and the City.

It is estimated that the cost to separate the Ottawa Public Library from the City's network would be $30,000 of one time capital funding and $150,000 of annual operating costs, including the funding of 1 additional FTE (or equivalent). A budget pressure will be identified for the 2007 budget.

Anti-Virus

Recommendation 6

That Information Technology Services:

- **Deploy the latest Symantec Antivirus version; and**
- **Update the configuration of the Anti-Virus systems includes anti-virus checking before file read and before program execution.**

Management Response

Management agrees with this recommendation.

IT Services considers that the risk of using the current version of Symantec Antivirus (7.61) is mitigated as three additional layers of anti-virus and malicious file protection also safeguard the City network, and Symantec continues to issue updated virus signature files per the support agreement up to January 31, 2006.

It is not uncommon for an organization of the size of the City of Ottawa to delay or skip version upgrades of software products. Upgrades are done either because the new functionality offered is needed by the City and is supported by a business case for the upgrade, or because the product is no longer supported by the vendor. IT Services has evaluated the additional features and business case for each new version as it is released. In fact, the City partnered with Symantec in Q1 2005 to beta-test version 10, as this is the first version to add features to safeguard against the current threat from spyware. Following this evaluation, Symantec recommended in late Q3 2005 that the City begin a managed upgrade directly from version 7.61 to Symantec Antivirus version 10.

IT Services initiated the upgrade to Symantec Antivirus 10 in Q4 2005, to be completed by January 31, 2006. This upgrade includes an assessment of the productivity impact of including anti-virus checking on read from disk and before program execution.

Log Management

Log management practices need to be improved. Effective log management allows an organization to detect malicious activity, understand current levels of events, and track trends of various operational

metrics. If was found that not all security device logs were being saved to permanent storage. It was also found that the logs that were collected were not routinely analyzed for significant events or trend analysis. Finally, the level of coverage of logging was not sufficient to record and detect all significant events on key security enforcement devices.

Recommendation 7

That Information Technology Services:

- **Review logging and monitoring processes and systems for effective operational system health and policy enforcement monitoring;**
- **Identify log events that require "real time" detection and alerting and implement appropriate processes;**
- **Review all security devices to ensure appropriate logging coverage;**
- **Ensure all device clocks are centrally synchronized for effective event correlation;**
- **Review regulatory and City policy requirements for an appropriate logging data retention period;**
- **Consider feeding log and monitoring data into a Security Information Management (SIM) tool for automated event analysis and correlation, to better provide a near real time City security posture;**
- **Ensure all devices are logging operational health and security events as a minimum; and**
- **Enable system logging on all devices.**

Management Response

Management does not completely agree with these recommendations.

Industry best practices do not support full logging on all devices at all times due to the high cost. IT Services implements additional logging and alerting on a selective basis, such as with certain high-risk devices or where there is a concern with a particular device.

As part of the Enterprise Security Review project initiated in Q1 2005, IT Services has contracted a third party security company to perform a detailed review of logging and monitoring processes and systems, including an assessment of the cost impact of these recommendations. The review will be completed in Q1 2006. If additional logging is required, a budget pressure will be identified in the 2007 budget. IT Services has implemented alerting for device failure on all servers and network devices.

IT Services has updated all firewalls to receive a synchronized time from NRC.

A review of regulatory and City policy requirements for logging data will be completed in Q2 2006, following the detailed review of logging and monitoring processes and systems in Q1 2006. Log data will be retained in accordance with the City's Records Management Policy and By-Law.

The need for additional logging and Security Information Management (SIM) tool will be assessed in Q2 2006 and if required a budget pressure will be identified in the 2007 budget. Additional logging is estimated to cost between $75,000-$150,000. To purchase and implement a SIM is $150,000, with

ongoing operating costs in excess of $200,000 per year. Ongoing FTE (or equivalent) requirements are unknown at this time.

Change Management

Change management process for security devices need to be improved and enforced. It was found that the existing change management process was not being followed for all devices. Therefore, a linkage is not available between the configurations on security devices and the requestor and approver of these configurations. This tracking is important for periodic security reviews.

Recommendation 8

That Information Technology Services:

- **Implement a more robust Change Management process/system within Corporate Services; and**
- **Enforce the formal Change Management process for all changes to the firewalls and other security systems.**

Management Response

Management agrees with these recommendations.

The current Change Management process in place since 2001 was enhanced in Q4 2005 to encompass all IT Services divisions and the requirement to comply with the City's Records Management Policy.

The Chief Information Officer reminded all IT Services Managers and Program Managers in November 2005, of the requirement to adhere to this Change Management process. This includes the requirement to document results achieved and record these centrally using the City's Records Management framework.

IT Security Policies

The IT Security policies were found to have some deficiencies in both content and interpretation. Not all users and systems were bound by the IT Security policies restricting use of the Internet. In particular, the Ottawa Public Library use of the Internet is governed by the requirement for intellectual freedom. The interpretation of this intellectual freedom results in various applications and services being installed for use by Library staff that bypass some of the controls implemented such as e-mail anti-virus filtering. Installation or configuration changes to access remote (i.e. on the Internet) data sources were also discovered on City workstations. In addition, the growing need to encrypt data to maintain confidentiality introduces the need to develop a policy to manage such encryption. Issues with encryption include key management (ensure that the ability to decrypt documents is maintained) and strength of encryption (ensure that the data or communication is sufficiently protected). The current IT Security policies state that encryption should be used to protect sensitive data, but don't currently address how this should be done.

Recommendation 9

That Information Technology Services ensure the policy prohibit the installation of software not officially sanctioned.

Management Response

Management agrees with this recommendation.

Section 6.4 of the revised Responsible Computing Policy, approved by City Management in September 2005, states: "Users shall not install or download software, shareware, freeware or any other application program onto City-owned IT assets without the express written permission of ITS."

Recommendation 10

That Information Technology Services ensure the policy prohibit the use of non-City approved computing resources for processing City data and assets.

Management Response

Management does not completely agree with this recommendation.

This recommendation applies to the following two situations:

- Use of non-City hardware by staff and/or consultants on the City network (e.g., laptops). Processing City data and assets using non-City hardware (e.g., home computers). IT Services concurs with the recommendation with respect to the use of non-City hardware on the City network (e.g., laptops). In section 6.3 of the revised Responsible Computing Policy, approved by City Management in September 2005, the Policy states: "Non-City hardware shall not be connected to the Corporate network without the express written consent of the ITS Branch."

- IT Services does not agree with this recommendation with respect to processing City data and assets using non-City hardware (e.g., home computers). Such a restriction would prohibit the use of web-mail from a home computer, or working from home on a Word document or Excel spreadsheet. The Responsible Computing Policy clearly defines employee obligations to safeguard electronic and information records in their custody, whether being processed at a City facility or not. The City's Defence-in-Depth Strategy mitigates the risk to the corporation from malicious software brought from a non-City computing environment.

Recommendation 11

That Information Technology Services review the retention periods for e-mail (including deleted e-mail) and compare to use of this data as corporate records and industry best practices.

Management Response

Management agrees with this recommendation.

The retention period for e-mail was reviewed against federal, provincial, and municipal legislation prior to approval of the Records Retention and Disposition By-law approved by Council and the Records Management Policy in 2003. Automated retention rules for e-mail were implemented as a part of an upgrade to the Exchange Server product in September 2005, to ensure compliance with this by-law and policy.

Recommendation 12

That Information Technology Services review the users with administrator rights on their workstations, and where not justified and required, remove the administrator privileges for that user.

Management Response

Management agrees with this recommendation.

A rigorous documented formal process is followed whenever any user requires local administrative rights.

As part of the Enterprise Security Review project, a review will be conducted regarding administrative access rights for IT Services with recommendations provided to the IT Services Management team in Q1 2006. This review will be repeated on an annual basis.

More restrictive administrative rights for laptop users are being implemented as part of the life cycle laptop replacement program. At this point, funding is available to replace roughly 100 units of the total fleet of 900.

Roughly 50% of the current fleet of City laptops are now running a version of the operating system that offers administrative rights control. IT Services plans to implement these administrative rights restrictions by the end of Q1 2006. The remaining 50% of the City laptop fleet needs to be replaced.

Funding of $700,000 and one (1) additional FTE (or equivalent) will be required in order to accelerate this replacement program to be completed over twelve (12) months. A budget pressure will be identified for the 2007 budget to accelerate this replacement program to be completed over twelve (12) months.

Recommendation 13

That Information Technology Services:

- **Review organization roles and responsibilities with accompanying agreements, such as Service Level Agreements (SLAs); and**
- **Clearly define roles/responsibilities and define processes to ensure control implementation and monitoring is covered.**

Management Response

Management disagrees with these recommendations.

IT Services has reviewed existing organizational roles and responsibilities, and believes that these roles and responsibilities are clearly delineated and effective. Separation of duties and other organizational control mechanisms are fully implemented and maintained across the entire branch.

Encryption Policy

Recommendation 14

That Information Technology Services develop an Encryption Policy to address key aspects of encryption related to the City's operations and requirements.

Management Response

Management agrees with this recommendation.

Encryption technologies are currently used to safeguard specific systems, but these *de facto* standards are not presently in one reference document. Existing encryption standards will be collected and documented by Q2 2006.

Recommendation 15

That Information Technology Services identify tools for encryption of sensitive e-mail content.

Management Response

Management disagrees with this recommendation.

The revised Responsible Computing Policy, section 7.1, as approved by City Management in September 2005 stipulates that sensitive information is not to be transmitted via the corporate e-mail system.

An enterprise wide e-mail encryption solution would be for internal use only and would not necessarily be compatible with external partners, as there is no national or international standard for e-mail encryption.

Should an enterprise-wide e-mail encryption solution be required, it is estimated to cost $100,000 and require 2 FTEs (or equivalent) to administer. A budget pressure would be identified for the 2007 budget.

Recommendation 16

That Information Technology Services implement strong encryption on the link between DC2 and the library lab network that uses the Internet for communication.

Management Response

Management agrees with this recommendation.

IT Security will investigate the use of this link and the safeguards currently in place in Q4 2005.

User IT Security Awareness

Recommendation 17

That Information Technology Services:

- **Create a program with annual user IT Security policy review with mandatory quarterly/semi-annually IT Security awareness briefings;**
- **Continue the Security flash e-mail awareness campaign notifying users of significant e-mail attacks; and**
- **Improve the effectiveness of the IT Security awareness campaign.**

Management Response

Management agrees with these recommendations.

A formal IT Security Awareness program already exists. Awareness articles are issued through City Briefs on a monthly basis, Management Bulletins are also issued as necessary, and IT Security awareness briefings occur to address strategic issues or groups. Awareness activities have been part of the annual planning cycle since 2003. Flash e-mail awareness campaigns will continue.

A third party review to measure and assess the current awareness targets and associated delivery strategy was scheduled to begin October 2005 as part of the Corporate IT Security Awareness Program. This review was deferred to 2006 due to a City-wide budget freeze, and will include specific recommendations and a workplan identifying the priority messaging targets

Internet Usage

The Internet policies should be revised to limit personal use of the Internet to incidental or occasional use only and compliance to the policies should be monitored. Overall, a large amount of the Internet usage was for personal use.

A sample of 50 random user accounts was scrutinized for the month of May 2005. The spread for this group ranged from 44,220 hits (or 2,106 hits per day for the highest user account) to no hits for the lowest user account. The review was based on a statistically valid sample and found that average personal use of the Internet for this group was 53%.

The Top 50 user accounts were scrutinized for the month of May 2005. The spread for this group differed greatly and ranged from 2,098,002 hits (or 99,905 hits per day for the highest user account) to 29,761 hits (or 1,417 hits per day for the lowest user account). We found that their average personal use of the Internet was 66%.

Below is the summary of Internet usage, as reported by Information Technology Services Branch, for the month of October 2005.

TOP 100 PERMITTED WEBSITES VISITED DURING OCTOBER 2005
Per Information Technology Services Branch

Category (per ITS)	Examples	% of Top 100 Website "hits"	% of Total Internet Traffic (Oct 2005)
Internet Search Engines	www.google.ca kh.google.com cdn.mapquest.com	41.7%	25.9%
Advertising	ad.doubleclick.net adcounter.theglobeandmail.com adme.411.ca	29.3%	18.2%
Sports, Shopping & Entertainment	www.tsn.ca www.mls.ca	5.3%	3.3%
News and Media	OttawaSun.com CBC.ca	4.2%	2.6%
References	weatheroffice.ec.gc.ca www.Isuc.on.ca	2.4%	1.5%
Job Search	Workopolis.com	2.0%	1.3%
Information Technology	download.windowsupdate.com www.microsolft.com	1.6%	1.0%
City of Ottawa Application	Interfleet.ca Library.Ottawa.on.ca	1.2%	0.7%
Other	Includes "uncategorized"	12.2%	7.6%
Totals		**99.9%**	**62.1%**

The Responsible Use of the Internet Policy regulates and provides direction for appropriate usage of the Internet to be observed by all users. During the course of our audit, we found non-compliance with the existing policy within the following areas:

- Usage, if subjected to public scrutiny, does not cause embarrassment or concern to the City;
- Access to non-City e-mail systems and accounts through the Internet (such as Hotmail) from City workstations is strictly prohibited;

- All employee use of the network and Internet is tracked and monitored;
- Users will not use the Internet for illegal or immoral purposes;
- Peer-to-Peer File Sharing;
- Web-chat;
- Internet auction;
- Shared accounts;
- Personal and Dating; and
- Personal Web Sites.

We were unable to conclude whether personal Internet usage by employees occurred during normal working hours, as Information Technology Services Branch did not provide the Office of the Auditor General with the "point in time" records.

Personal e-mail usage was not as high as that of the Internet**.** Based on a sample of 50 random users, approximately 16% of e-mails were found to be personal. All users had at least some business requirement for e-mail use.

An analysis of the top 50 e-mail users could not be performed, as Information Technology Services was unable to generate an accurate report. We would expect that an organization such as the City of Ottawa would have proven tools to accurately and quickly provide reports such as top e-mail users, random users, sent e-mails, received e-mails, and other e-mail metrics to be used to analyze e-mail usage. Alternative methods to track and monitor high e-mail users should be obtained.

The Responsible Use of the Internet Policy specifically allows personal use of this corporate resource. While it may be expected that some minimum level of incidental personal usage may occur, we would expect that the level of personal use of the Internet should be similar to the expectations of limited personal use of the telephone. The City's policy on e-mail use only permits incidental personal use of e-mail, similar to the expectation of limited telephone use. Given the high personal use of Internet we found, the City's Responsible Use of the Internet Policy should be revised to limit personal use of the Internet to incidental or occasional only.

In order for managers to monitor staff to ensure that they are using Internet and e-mail appropriately, managers need to be provided with reports of Internet and e-mail usage. Information Technology Services is responsible for monitoring and controlling the use of the Internet and e-mail. This should include a process for reporting high volume or unusual usage patterns to managers so that they may evaluate if appropriate usage has occurred.

Currently, Information Technology Services does not provide regular reports of use of Internet or e-mail to departmental managers for review to ensure staff is using these tools appropriately. Monitoring can be accomplished through a process to provide reports to management for these reviews.

Policy Compliance – Internet and E-mails

Recommendation 18

That Information Technology Services:

- **Monitor and control the use of the Internet and e-mail usage by City employees;**
- **Develop appropriate recording tools that provide reliable reporting of e-mail usage;**

- **Develop and implement a process to provide managers with reports of their staff's Internet and e-mail usage so that management can evaluate if appropriate usage of e-mail and Internet is occurring; and**
- **Revise the Responsible Computing Policy to limit use of the Internet to mainly business purposes and limit personal usage to incidental or occasional only.**

Management Response

Management agrees with these recommendations.

IT Services uses Websense to monitor and control the use of the Internet at a macro or system level. Prior to the audit, IT Services launched an extensive project to enhance the rigour of the Websense implementation, scheduled for completion in Q1 2006. An extensive range of additional Websense filtering features is now in place that enhances the monitoring of Internet usage and blocking of websites that are not consistent with the Code of Conduct and Responsible Computing Policy. Monthly reviews of Websense reports by IT Services will continue, and changes to categories, website blocking, and follow-up investigations will continue.

In 2006 IT Services will enhance Internet monitoring using existing Websense reporting tools. A detailed analysis of a minimum of 50 Internet accounts will be conducted on a semi-annual basis for compliance with the Responsible Computing Policy. Instances of non-compliance will be investigated in conjunction with managers and the Labour Relations unit within Employee Services Branch. It is projected that this level of review and follow-up will generate the equivalent of 1.5 FTEs (2,700 hours) of staff effort to implement.

IT Services/Labour Relations will be contacting the respective managers of the 50 random and 50 top users generated throughout the audit. IT Services in consultation with Labour Relations will provide the Internet log report along with guidelines on how to interpret the data set and how to approach employees with any concerns that might be presented on their Internet usage.

IT Services will continue to produce management reports and metrics using Promodag, and will investigate additional monitoring tools and reporting capabilities that would enable monitoring of individual e-mail accounts. Evidence of non-compliance with the Responsible Computing Policy will be investigated in conjunction with managers and Labour Relations. At this time, the additional effort to review and follow-up is not known pending identification and selection of new tools. A budget pressure would be identified for 2007 to acquire and implement additional monitoring and reporting tools.

The revised Responsible Computing Policy clearly states that the Internet and e-mail are provided for "legitimate business use in the course of assigned duties and only incidentally for personal use", and that disciplinary action, including dismissal, are consequences of non-compliance. The Responsible Computing Policy will be reviewed to ensure that it applies equally to both Internet usage and e-mail usage, and reflects our current practices.

Overall Management Comments

Information Technology Services (ITS) concurs with many of the recommendations proposed by the Auditor General. Where Management does not agree with the findings and/or recommendations proposed by the Auditor General, an explanation is provided to substantiate this position. In all cases, this is the result of further research or consultation with vendor suppliers, security experts, and industry best practices.

In cases where Management has already commenced an action, a status update has been provided. Where no action has been taken, the proposed timeline and any budgetary implications and expected outcomes have been identified.

1.6 Conclusion

This audit reviewed the adequacy, effectiveness and reliability of security measures and controls in place over the usage of the Internet and e-mail and assessed whether usage is compliant with City policies. While security controls currently implemented were found to be generally effective and reliable, there were gaps in the adequacy of the controls. The audit also reviewed the compliance of usage of the Internet and e-mail to the current policy statements and found that there is considerable personal use of these tools. The Responsible Use of the Internet Policy and the Responsible Computing Policy should be revised to limit the use of the Internet to mainly business purposes and limit personal usage to incidental or occasional only. A program to monitor and control Internet and e-mail usage should also be established.

We wish to express our appreciation for the cooperation and assistance afforded the audit team by Management.

Résumé

1.0 Introduction

La vérification de l'utilisation et de contrôles d'Internet était incluse dans le plan de vérification de 2005 proposé par le vérificateur général de la Ville et reçu par le Conseil municipal le 15 décembre 2004.

1.1 Contexte

La Ville d'Ottawa compte environ 9 000 internautes. Tous ces utilisateurs ont accès à la messagerie électronique, au Web ainsi qu'à d'autres protocoles de communication Internet (par exemple, le logiciel de clavardage en ligne MSN Messenger, le protocole FTP et les protocoles spécialisés des systèmes de classification des bibliothèques) au sein de la Ville d'Ottawa. Pour faciliter cette communication et le transfert d'information connexe, la Ville offre 220 connexions Internet haute vitesse et 60 accès par ligne commutée.

La Direction des services de technologie de l'information a signalé qu'au total, 26,7 millions de requêtes avaient été effectuées sur Internet par les 6 226 utilisateurs l'ayant utilisé en octobre 2005, ce qui représente une moyenne de 4 282 requêtes par utilisateur pour ce mois.

Les systèmes de courriel de la Ville transfèrent chaque jour plus de 200 000 courriels.

L'utilisation des services Internet et des services de courriel de la Ville est réglementée et régie par deux (2) politiques. Aux fins de la présente vérification, nous avons examiné les politiques suivantes, en vigueur au moment de notre examen.

- Utilisation responsable des ordinateurs - politique municipale (13 août 2001); et
- Politique sur l'utilisation responsable de l'Internet (11 décembre 2003).

En raison de son besoin de flexibilité et d'un filtrage moins restrictif du contenu Internet et du contenu de courriels, la Bibliothèque publique d'Ottawa (BPO) profite d'une application moins stricte des contrôles de sécurité.

1.2 Portée de la vérification

La portée de la vérification se limite à la stratégie, aux politiques, aux procédures et aux autres contrôles de technologie de l'information (TI) (y compris les outils techniques) qui définissent et limitent l'utilisation d'Internet par la Ville d'Ottawa. Les points suivants ont notamment été examinés :

- stratégie de sécurité de la de la Gestion de l'information des Services de technologies de l'information (GI/TI);
- politiques d'utilisation responsable;
- politiques d'enquêtes sur les incidents;
- politiques de demandes de services;
- coupe-feu;
- filtrage anti-pourriel;
- filtrage antivirus;
- filtrage de contenu;

- 8 grands sites et 6 petits sites municipaux;
- conformité du trafic Internet (sites consultés) avec la Politique d'utilisation responsable de l'Internet;
- conformité de l'utilisation du courriel avec la politique.

Le Service de police d'Ottawa n'étaient pas inclus dans cette vérification.

1.3 Objectif de la vérification

La vérification vise à fournir une évaluation indépendante et objective pour :

- évaluer la suffisance, l'efficacité et la fiabilité de la stratégie, de la politique, des mesures et des contrôles de sécurité en place pour l'utilisation d'Internet et du courriel; et
- déterminer si l'utilisation d'Internet et du courriel est conforme aux politiques municipales.

1.4 Principales constatations et recommandations

Les principales constatations et recommandations de la présente vérification peuvent être ainsi résumées.

Dans l'ensemble, les contrôles de courriels visant à protéger la confidentialité, l'intégrité et la disponibilité des systèmes et de l'information fonctionnaient comme prévu. Plus particulièrement, nous avons conclu à l'efficacité des contrôles de sécurité visant l'isolation des pièces jointes dangereuses incluses dans les courriels. Bien que des utilisateurs avertis aient pu passer outre les contrôles de blocage par type de fichier, ils ne pouvaient contourner les contrôles antivirus puisque neuf moteurs antivirus bloquaient le contenu des fichiers malveillants.

Nous avons cependant conclu que le verrouillage des ordinateurs de bureau publics, dans les bibliothèques et centres d'emploi, pourrait être sensiblement amélioré si la correction de programme automatisée de Windows XP et la plus récente version de Symantec Antivirus étaient installées sur ces derniers.

Enfin, nous avons jugé que la mise en place du coupe-feu anti-pourriel en janvier 2004 avait sensiblement réduit la quantité de pourriels que doit traiter le personnel de la Ville. Cela a également réduit le risque que les pourriels déclenchent une attaque logicielle malveillante, en plus de réduire les exigences en matière de ressource de système pour l'envoi et la réception du courriel.

Recommandation 1

Que les Services de technologie de l'information examinent les outils utilisés pour effectuer le blocage par type de fichier, pour ainsi activer cette fonction, quelle que soit l'extension du fichier.

Recommandation 2

Que les Services de technologie de l'information déploient la plus récente version de Symantec Antivirus.

Recommandation 3

Que les Services de technologie de l'information mettent à jour la configuration des systèmes antivirus pour y inclure un contrôle antivirus qui s'activerait au moment de l'extraction de fichiers et avant l'exécution d'un programme.

Réponse de la direction

La direction est d'accord avec les recommandations 1, 2 et 3.

Les Services de TI examinent en ce moment une nouvelle fonction, disponible depuis peu, pour la première couche de protection associée à la détection de virus. Elle permettrait de bloquer certains types de fichiers, quelle que soit l'extension de ces derniers. Des essais seront effectués pendant le premier trimestre de 2006 pour ainsi s'assurer que ce logiciel ne nuira pas à l'envoi et à la réception de courriels.

Les Services de TI jugent que le risque posé par l'utilisation de la version actuelle de Symantec Antivirus (7.61) est limité. En effet, le réseau municipal est également protégé par trois couches supplémentaires de protection contre les virus et fichiers malveillants, et Symantec continue d'émettre les mises à jour des fichiers de signatures de virus, conformément à l'entente de soutien, jusqu'au 31 janvier 2006.

Il n'est pas inhabituel qu'une organisation de la taille de la Ville d'Ottawa retarde ou saute des mises à niveau logicielles. Ces mises à niveau sont effectuées soit parce que la Ville a besoin de la nouvelle fonctionnalité offerte et qu'une analyse de rentabilisation appuie cette mise à niveau, soit parce que le fournisseur n'offre plus de soutien pour le produit visé. Les Services de TI évaluent les nouvelles caractéristiques et l'analyse de rentabilité pour toutes les nouvelles versions et ce, au moment de leur lancement. En fait, la Ville s'est associée à Symantec au premier trimestre de 2005 pour procéder à un essai bêta de la version 10 puisque cette version était la première à ajouter des fonctions de protection contre la menace posée par les logiciels espions. À la suite de cette évaluation, Symantec a recommandé, vers la fin du troisième trimestre de 2005, que la Ville entame une mise à niveau gérée pour passer directement de la version 7.61 à la version 10 de Symantec Antivirus.

Au quatrième trimestre de 2005, les Services de TI ont entamé la mise à niveau pour passer à la version 10 de Symantec Antivirus, mise à niveau qui doit être terminée avant le 31 janvier 2006. Cette mise à niveau comprend une évaluation des répercussions sur la productivité qu'aurait l'ajout d'un contrôle antivirus pendant l'extraction des fichiers et avant l'exécution d'un programme.

Recommandation 4

Que les Services de technologie de l'information,

- **examinent le niveau de sensibilisation des utilisateurs par rapport à la boîte de pourriels et au besoin en augmentent la visibilité au besoin;**
- **continuent de surveiller l'efficacité des outils actuels de filtrage des pourriels.**

Réponse de la direction

La direction est d'accord avec cette recommandation.

L'adresse spam@ottawa.ca continue d'être incluse dans le programme permanent de sensibilisation à la sécurité mis en place par les Services de TI. Chaque mois, plus de 1 000 courriels reçus de l'externe par le personnel de la Ville sont envoyés à la boîte de pourriels pour examen. De plus, quatre articles « La ville en bref » ont été publiés en 2005 sur le thème des pourriels et chacun comportait un rappel sur la disponibilité de cette adresse. Les Services de TI vont continuer à rappeler régulièrement au personnel l'existence de la boîte de pourriels.

Quand elles sont disponibles auprès du fournisseur, les mises à niveau du service de filtrage des pourriels sont effectuées par les Services de TI pour garantir l'efficacité continue de ce service. Comme il est indiqué dans le rapport, le service de filtrage des pourriels est surveillé chaque jour et examiné chaque mois par les Services de TI.

Les données de MessageLabs indiquent qu'en octobre, 65 % de tous les messages envoyés dans le monde étaient des pourriels. Des 50 000 messages reçus chaque jour de l'externe par les 9 000 utilisateurs de la messagerie électronique de la Ville, un peu plus de 50 % sont jugés être des pourriels et sont immédiatement rejetés. Environ 0,5 % de ces messages sont des pourriels qui ne sont pas identifiés ni rejetés et parviennent donc jusqu'à un destinataire de la Ville. Cela représente 250 messages par jour pour l'ensemble de la Ville. Les utilisateurs sont encouragés à transmettre les pourriels aux Services de TI afin de contribuer à l'amélioration de l'efficacité du service de filtrage.

Filtrage site Web - Protocol HTTP

Alors que l'outil de filtrage de contenu Websense est généralement jugé efficace, il met également en lumière une faiblesse fondamentale de la position globale de la Ville en matière de sécurité. Le réseau municipal est un ensemble homogène de dispositifs non séparés les uns des autres par des contrôles de sécurité. Ainsi, si un incident de sécurité se produit, tous les systèmes du réseau pourront rapidement être touchés. Le modèle de sécurité de la Ville repose sur une sécurité périmétrique robuste qui contribue à la prévention de tels incidents. La majorité des utilisateurs du réseau municipal sont protégés par une gamme de dispositifs de sécurité préventive liés en grande partie au périmètre. Les utilisateurs de la Bibliothèque publique d'Ottawa sont partiellement exemptés de certains de ces contrôles. Il en découle donc que les contrôles robustes de sécurité périmétrique peuvent être annulés, ce qui pourrait permettre à des programmes malveillants de pénétrer le réseau municipal. Ce contournement de certains contrôles est une faiblesse de la sécurité de la Ville.

Recommandation 5

Que les Services de technologie de l'information resserrent la mise en œuvre du service Websense pour ainsi réduire la possibilité de contourner ce service.

Réponse de la direction

La direction est d'accord avec cette recommandation.

En 2005, avant la vérification, les Services de TI avaient lancé un vaste projet, devant se terminer au cours du premier trimestre de 2006, et visant à utiliser Websense de façon plus rigoureuse. Au moment où nous rédigeons la présente réponse (novembre 2005), une vaste gamme de fonctions de filtrage Websense supplémentaires a déjà été mise en place.

Les constatations de la vérification ont permis d'identifier un petit site (le Centre communautaire Don-Gamble) qui permettait au personnel de la Ville d'Ottawa d'avoir accès à Internet sans filtrage. Ainsi, un problème de routage de sous-réseau indiquait à Websense que ces quatre employés municipaux travaillaient sur des postes de la Bibliothèque non visés par le filtrage (voir ci-dessous). Les Services de TI ont corrigé ce problème.

- **Que les Services de technologie de l'information examinent la possibilité de fixer, pour la bibliothèque, un certain degré de filtrage, comme un nombre limité de systèmes à usage général isolés offrant un accès non filtré à Internet, pour ainsi réduire les risques. Si cela ne peut être accompli au niveau approprié, les Services de technologie de l'information devraient alors songer à isoler la Bibliothèque publique d'Ottawa du système municipal.**

Réponse de la direction

Le personnel de la Bibliothèque publique d'Ottawa (BPO) bénéficie d'un accès non filtré à Internet pour des raisons de liberté intellectuelle. Puisque cela découle d'une directive du Conseil de la Bibliothèque et constitue donc une question de gouvernance liée au Conseil de la Bibliothèque, elle n'est pas du ressort de la Direction des services de TI.

Depuis 2001, d'importants efforts ont été réalisés par les Services de TI pour gérer les risques que posait cette configuration. Ainsi, les postes de travail de la bibliothèque se trouvent sur des segments de réseau distincts, ce qui facilite l'isolement des virus, des vers et des logiciels espions en cas d'irruption de programmes malveillants. Sur les conseils du personnel des Services de TI, la direction de la bibliothèque a consenti, en octobre 2005, à autoriser ces Services à protéger les postes de travail contre les programmes malveillants circulant sur Internet. Les postes de travail utilisés par les membres du personnel de la bibliothèque ne permettent pas l'accès à des sites malveillants. Cependant, l'accès à tous les autres sites reste entièrement libre, sans filtrage.

Puisque la BPO est régie par le Conseil de la Bibliothèque, il ne sera peut-être pas possible d'inciter ce dernier à revenir sur sa décision de permettre un accès illimité aux sites Internet en raison du principe de liberté intellectuelle. Ainsi, s'il est impossible d'appliquer un filtrage à un degré raisonnable, la Direction des services de TI est d'accord avec à la recommandation selon laquelle il faudrait songer à isoler la Bibliothèque publique d'Ottawa du système municipal. Cela constituerait une opération d'importance puisque la Bibliothèque publique d'Ottawa (BPO) offre 33 sites, répartis dans toute la ville. En outre, isoler la Bibliothèque publique d'Ottawa du réseau de la Ville d'Ottawa engagerait des frais supplémentaires non négligeables puisque la BPO et la Ville partagent certaines applications de gestion et ressources des Services de TI.

L'on estime qu'isoler la Bibliothèque publique d'Ottawa du réseau municipal coûterait 30 000 $ en capital de départ et 150 000 $ en charge d'exploitation annuelles, y compris le financement d'un ÉTP supplémentaire (ou l'équivalent). Une pression budgétaire sera indiquée dans le budget de 2007.

Antivirus

Recommandation 6

Que les Services de technologie de l'information,

- **déploient la plus récente version de Symantec Antivirus;**
- **mettent à jour la configuration des systèmes antivirus pour inclure un contrôle antivirus pendant l'extraction des fichiers et avant l'exécution d'un programme.**

Réponse de la direction

La direction est d'accord avec cette recommandation.

Les Services de TI jugent que le risque posé par l'utilisation de la version actuelle de Symantec Antivirus (7.61) est limité. En effet, le réseau municipal est également protégé par trois couches supplémentaires de protection contre les virus et fichiers malveillants, et Symantec continue d'émettre les mises à jour des fichiers de signatures de virus, conformément à l'entente de soutien, jusqu'au 31 janvier 2006.

Il n'est pas inhabituel qu'une organisation de la taille de la Ville d'Ottawa retarde ou saute des mises à niveau logicielles. Ces mises à niveau sont effectuées soit parce que la Ville a besoin de la nouvelle fonctionnalité offerte et qu'une analyse de rentabilité appuie cette mise à niveau, soit parce que le fournisseur n'offre plus de soutien pour le produit visé. Les Services de TI évaluent les nouvelles caractéristiques et l'analyse de rentabilité pour toutes les nouvelles versions et ce, au moment de leur lancement. En fait, la Ville s'est associée à Symantec au premier trimestre de 2005 pour procéder à un essai bêta de la version 10 puisque cette version était la première à ajouter des fonctions de protection contre la menace posée par les logiciels espions. Après cette évaluation, Symantec a recommandé, vers la fin du troisième trimestre de 2005, que la Ville entame une mise à niveau gérée pour passer directement de la version 7.61 à la version 10 de Symantec Antivirus.

Au quatrième trimestre de 2005, les Services de TI ont entamé la mise à niveau pour passer à la version 10 de Symantec Antivirus, mise à niveau qui doit être terminée avant le 31 janvier 2006. Cette mise à niveau comprend une évaluation des répercussions sur la productivité qu'aurait l'ajout d'un contrôle antivirus pendant l'extraction des fichiers et avant l'exécution d'un programme.

Gestion des journaux

Les pratiques de gestion des journaux doivent être améliorées. Une gestion efficace de ces journaux permet à une organisation de détecter les activités malveillantes, de comprendre les niveaux actuels des événements et de suivre les tendances à l'égard de différentes mesures d'exploitation. L'on a constaté que les journaux des différents dispositifs de sécurité n'étaient pas tous conservés dans une mémoire permanente. Il a également été noté que les journaux recueillis ne faisaient pas l'objet d'analyses de routine permettant d'analyser les événements ou tendances notables. Enfin, le degré de

couverture de la journalisation n'était pas suffisant pour enregistrer et détecter tous les événements importants liés aux dispositifs principaux d'application des mesures de sécurité.

Recommandation 7

Que les Services de technologie de l'information,

- **examinent les processus et systèmes de journalisation et de surveillance pour assurer un fonctionnement efficace et sain du système opérationnel et une surveillance de l'application des politiques,**
- **identifient les événements journalisés qui exigent une détection et une alerte en « temps réel » et que soient mis en œuvre les processus appropriés,**
- **examinent tous les dispositifs de sécurité pour ainsi garantir une journalisation et une couverture appropriées,**
- **s'assurent que les horloges de tous les dispositifs font l'objet d'une synchronisation centralisée pour assurer une corrélation efficace des différents événements,**
- **examinent toutes les exigences réglementaires et exigences connexes aux politiques municipales pour assurer une période appropriée de conservation des données de journalisation,**
- **songent à transmettre les données de journalisation et de surveillance à l'outil de gestion de la sécurité de l'information pour ainsi obtenir une analyse et une corrélation automatisées des événements et fournir à la Ville une meilleure image de la sécurité en temps quasi réel,**
- **garantissent que tous les dispositifs assurent au minimum la journalisation des événements connexes à la santé et la sécurité des systèmes,**
- **activent la journalisation pour tous les dispositifs.**

Réponse de la direction

La direction n'ait pas entièrement d'accord avec ces recommandations.

Les meilleures pratiques de l'industrie n'encouragent pas la journalisation complète et en tout temps de tous les dispositifs et ce, en raison du coût élevé d'une telle opération. Les Services de TI effectuent une journalisation et un alertage sélectifs, notamment pour certains dispositifs très vulnérables ou lorsqu'un certain dispositif soulève des inquiétudes.

Dans le cadre du projet d'examen de la sécurité d'entreprise (Enterprise Security Review) entamé au premier trimestre de 2005, les Services de TI ont signé un contrat avec une entreprise de sécurité chargée d'effectuer un examen détaillé des processus et des systèmes de journalisation et de surveillance, y compris une évaluation des répercussions financières de ces recommandations. Cet examen se terminera pendant le premier trimestre de 2006. Si un élargissement de la journalisation est requis, une pression budgétaire sera indiquée dans le budget de 2007. Les Services de TI ont mis en place un système d'alerte en cas de défaillance des dispositifs pour tous les serveurs et périphériques de réseau.

Les Services de TI ont aussi mis à jour les coupe-feu pour qu'ils utilisent l'heure synchronisée du CNRC.

Un examen des exigences réglementaires et des exigences connexes aux politiques municipales concernant les données de journalisation sera achevé au deuxième trimestre de 2006, après l'examen

détaillé des processus et des systèmes de journalisation et de surveillance du premier trimestre de 2006. Les données de journalisation seront conservées en conformité avec la Politique de gestion des dossiers de la Ville et avec les règlements municipaux en la matière.

Le besoin d'élargissement de la journalisation, ainsi que l'outil de gestion de la sécurité de l'information seront évalués pendant le deuxième trimestre de 2006 et, le cas échéant, une pression budgétaire sera indiquée dans le budget de 2007. L'on estime qu'un élargissement de la journalisation coûterait de 75 000 à 150 000 $. L'achat et la mise en œuvre d'un outil de gestion de la sécurité de l'information atteindraient 150 000 $ alors que les coûts d'exploitation continus dépasseraient les 200 000 $ par an. Les exigences liées à un ÉTP (ou l'équivalent) continu ne sont pas encore connues.

Gestion du changement

Le processus de gestion du changement connexe aux dispositifs de sécurité doit être amélioré et renforcé. L'on a constaté que les dispositifs ne respectaient pas tous le processus existant de gestion du changement. Par conséquent, il n'y a aucun lien entre les configurations des dispositifs de sécurité et le demandeur et l'approbateur de ces configurations. Ce suivi est important pour les examens périodiques en matière de sécurité.

Recommandation 8

Que les Services de technologie de l'information,

- **mettent en œuvre un processus/système de gestion du changement plus robuste au sein des Services généraux;**
- **appliquent le processus officiel de gestion du changement à tous les changements effectués sur les coupe-feu et autres systèmes de sécurité.**

Réponse de la direction

La direction est d'accord avec ces recommandations.

Le processus actuel de gestion du changement, en place depuis 2001, a été amélioré au quatrième trimestre de 2005 pour englober toutes les divisions des Services de TI, ainsi que les exigences de conformité avec la Politique de gestion des dossiers de la Ville.

En novembre 2005, le chef de l'information a rappelé à tous les gestionnaires de services de TI et aux gestionnaires de programmes la nécessité de se conformer à ce processus de gestion du changement. Cela inclut l'exigence de documenter les résultats obtenus et de les consigner de façon centralisée selon le cadre de gestion des dossiers de la Ville.

Politiques de sécurité des TI

L'on a constaté que les politiques de sécurité des TI comportaient certaines carences au niveau du contenu et de l'interprétation. Tous les utilisateurs et systèmes n'étaient pas liés par les politiques de sécurité des TI restreignant l'utilisation d'Internet. De façon plus particulière, l'utilisation d'Internet par la Bibliothèque publique d'Ottawa est régie par l'exigence de liberté intellectuelle. Il découle de l'interprétation de cette liberté intellectuelle que différents services et applications installés pour être

utilisés par le personnel de la bibliothèque passent outre certains des contrôles, comme le filtrage antivirus du courriel. Des modifications apportées à l'installation ou à la configuration pour permettre l'accès à distance (sur Internet) à des sources de données ont également été découvertes sur des postes de travail municipaux. En outre, le besoin croissant de crypter les données pour conserver la confidentialité crée le besoin d'élaborer une politique de gestion de ce cryptage. Certaines des questions liées au cryptage incluent la gestion des clés (garantir le maintien de la capacité à décrypter les documents) et la solidité du cryptage (garantir que les données ou les communications sont suffisamment protégées). Dans leur forme actuelle, les politiques de sécurité des TI indiquent que le cryptage doit être utilisé pour protéger les données confidentielles, mais elles ne précisent pas la façon dont cela doit être fait.

Recommandation 9

Que les Services de technologie de l'information s'assurent que la politique interdit l'installation de logiciels n'ayant pas reçu d'approbation officielle.

Réponse de la direction

La direction est d'accord avec cette recommandation.

La section 6.4 de la version révisée de l'Utilisation responsable des ordinateurs - politique municipale, approuvée par la direction de la Ville en septembre 2005, prévoit : « Il est interdit aux utilisateurs de télécharger ou d'installer des logiciels, des partagiciels, des gratuiciels ou toute autre application sur les ressources informatiques de la Ville sans en avoir obtenu au préalable l'autorisation écrite des STI. »

Recommandation 10

Que les Services de technologie de l'information s'assurent que la politique interdit d'utiliser des ressources informatiques non approuvées par la Ville pour le traitement de données et d'actifs municipaux.

Réponse de la direction

La direction n'ait pas entièrement d'accord avec cette recommandation.

Cette recommandation s'applique aux deux situations suivantes :

- L'utilisation, sur le réseau municipal, par du personnel ou des consultants, de matériel n'appartenant pas à la Ville (par ex., ordinateurs portables). Traitement de données et d'actifs municipaux avec du matériel n'appartenant pas à la Ville (par ex., ordinateurs domestiques). Les Services de TI approuvent cette recommandation en ce qui a trait à l'utilisation, sur le réseau municipal, de matériel n'appartenant pas à la Ville (par ex., ordinateurs portables). La section 6.3 de la version révisée de l'Utilisation responsable des ordinateurs - politique municipale, approuvée par la direction de la Ville en septembre 2005, prévoit : « Aucun matériel n'appartenant pas à la Ville ne doit être connecté à son réseau sans une autorisation écrite des STI à cet effet. »

- Les Services de TI n'approuvent pas cette recommandation en ce qui a trait au traitement de données et d'actifs municipaux avec du matériel n'appartenant pas à la Ville (par ex.,

ordinateurs domestiques). Une telle restriction interdirait l'utilisation de messageries électroniques depuis un ordinateur domestique ou le travail à domicile sur un document Word ou une feuille de calcul Excel. La Politique d'activité informatique responsable définit clairement les obligations des employés quant aux mesures de protection qui doivent être prises à l'égard des documents et des renseignements informatiques dont ils ont la garde, que ceux-ci soient traités dans un établissement municipal ou non. La stratégie municipale de défense en profondeur atténue le risque pour la municipalité que posent les logiciels malveillants provenant d'environnements informatiques autres que municipaux.

Recommandation 11

Que les Services de technologie de l'information examinent les périodes de conservation du courriel (y compris des messages supprimés) et les comparent à l'utilisation de ces données en tant que documents municipaux ainsi qu'aux meilleures pratiques de l'industrie.

Réponse de la direction

La direction est d'accord avec cette recommandation.

La période de conservation du courriel a été examinée en regard des lois fédérales, provinciales et municipales, avant l'approbation du Règlement sur la conservation et le déclassement des dossiers, approuvé par le Conseil municipal, et de la Politique de gestion des documents, en 2003. Les règles de conservation automatisée des courriels ont été mises en œuvre en septembre 2005 dans le cadre d'une mise à niveau du produit Exchange Server, pour garantir la conformité avec ce règlement et cette politique.

Recommandation 12

Que les Services de technologie de l'information examinent la liste des utilisateurs possédant des droits d'administrateur sur leur poste de travail, et retirent les privilèges de gestion des utilisateurs pour lesquels ils ne sont ni justifiés ni requis.

Réponse de la direction

La direction est d'accord avec cette recommandation.

Une procédure officielle documentée et rigoureuse est suivie chaque fois qu'un utilisateur demande des droits locaux de gestion de réseau.

Dans le cadre du projet d'examen de la sécurité d'entreprise, un examen sera effectué à l'égard des droits d'accès à la gestion de réseau des Services de TI, et des recommandations seront présentées à l'équipe de direction des Services de TI au premier trimestre de 2006. Cet examen sera effectué tous les ans.

Dans le cadre du programme de remplacement des ordinateurs portables lié à leur cycle de vie, des droits d'administrateur plus restrictifs sont actuellement mis en place pour les utilisateurs d'ordinateurs portables. À l'heure actuelle, un budget est offert pour le remplacement d'environ 100 unités, dans un parc comptant un total de 900 unités.

Environ 50 % des ordinateurs portables du parc actuel de la Ville utilisent un système d'exploitation permettant de contrôler les droits d'administrateur. Les Services de TI prévoient mettre en œuvre ces restrictions des droits d'administrateur avant la fin du premier trimestre de 2006. Les 50 % restants du parc municipal d'ordinateurs portables doivent être remplacés.

Un budget de 700 000 $ ainsi qu'un budget pour un (1) ÉTP (ou l'équivalent) supplémentaire seront nécessaires pour accélérer ce programme de remplacement, pour qu'ainsi, il puisse être effectué en douze (12) mois. Une pression budgétaire sera indiquée dans le budget de 2007 pour accélérer ce programme de remplacement afin qu'il puisse être terminé en douze (12) mois.

Recommandation 13

Que les Services de technologie de l'information,

- **examinent les rôles et responsabilités de l'organisation, ainsi que les ententes s'y rattachant, telles les ententes sur les niveaux de service (ENS);**
- **définissent clairement les rôles/responsabilités, ainsi que des processus pour garantir que l'application et la surveillance des contrôles sont couvertes.**

Réponse de la direction

La direction n'ait pas d'accord avec ces recommandations.

Les Services de TI ont examiné les rôles et responsabilités existants dans l'organisation et croient que ces rôles et responsabilités sont clairement délimités et efficaces. La répartition des responsabilités et les autres mécanismes de contrôle organisationnels sont entièrement mis en œuvre et maintenus dans l'ensemble de la Direction.

Politique de cryptage

Recommandation 14

- **Que les Services de technologie de l'information élaborent une politique de cryptage visant les principaux aspects du cryptage, à l'égard des activités et des besoins de la Ville.**

Réponse de la direction

La direction est d'accord avec cette recommandation.

Des technologies de cryptage sont actuellement utilisées pour protéger des systèmes particuliers, mais ces normes *de facto* ne sont pas consignées dans un document de référence unique. Les normes de cryptage existantes seront recueillies et documentées avant le deuxième trimestre de 2006.

Recommandation 15

- **Que les Services de technologie de l'information identifient des outils de cryptage des courriels à contenu délicat.**

Réponse de la direction

La direction n'est pas d'accord avec cette recommandation.

La section 7.1 de la version révisée de l'Utilisation responsable des ordinateurs - politique municipale, telle qu'elle a été approuvée par la direction de la Ville en septembre 2005, prévoit qu'aucun renseignement de nature délicate ne doit être transmis via le système de courriel municipal.

Une solution de cryptage du courriel utilisée dans l'ensemble de la Ville ne serait qu'à usage interne et ne serait pas nécessairement compatible avec des partenaires externes, puisqu'il n'y a aucune norme nationale ou internationale pour le cryptage du courriel.

Si une solution de cryptage du courriel appliquée à toute l'entreprise était requise, l'on estime qu'elle coûterait 100 000 $ et que son administration demanderait 2 ÉTP (ou l'équivalent). Une pression budgétaire serait indiquée dans le budget de 2007.

Recommandation 16

- **Que les Services de technologie de l'information mettent sur pied un cryptage résistant sur le lien entre le gestionnaire de périphérique 2 et le réseau laboratoire de la bibliothèque qui utilise Internet pour ses communications.**

Réponse de la direction

La direction est d'accord avec cette recommandation.

Au quatrième trimestre de 2005, la Sécurité des TI va étudier l'utilisation de ce lien et les mesures de protection actuellement en place.

Sensibilisation des utilisateurs à la sécurité des TI

Recommandation 17

Que les Services de technologie de l'information,

- **créent un programme comprenant un examen annuel de la politique sur la sécurité des TI vis-à-vis des utilisateurs, et des séances trimestrielles/semestrielles obligatoires de sensibilisation à la sécurité des TI,**
- **poursuivent leur campagne de sensibilisation à la sécurité par courriel Flash, en avertissant les utilisateurs des attaques majeures transmises par courriel;**
- **améliorent l'efficacité de la campagne de sensibilisation à la sécurité des TI.**

Réponse de la direction

La direction est d'accord avec cette recommandation.

Un programme officiel de sensibilisation à la sécurité des TI existe déjà. Des articles de sensibilisation sont publiés tous les mois, dans « La ville en bref ». Des Bulletins des gestionnaires sont également publiés au besoin, et des séances de sensibilisation à la sécurité des TI sont tenues et abordent des questions ou s'adressent à des groupes stratégiques. Des activités de sensibilisation sont incluses dans le cycle de planification annuel depuis 2003. Les campagnes de sensibilisation par courriel Flash vont se poursuivre.

Il a été prévu qu'un examen indépendant visant à mesurer et à évaluer les cibles actuelles de sensibilisation et la stratégie de communication connexe commencera en octobre 2005, dans le cadre du Programme municipal de sensibilisation à la sécurité des TI. Cet examen a été reporté en 2006 en raison d'un gel budgétaire à l'échelle de la ville. Il inclura des recommandations précises ainsi qu'un plan de travail identifiant les cibles prioritaires des messages.

Utilisation d'Internet

Les politiques portant sur Internet doivent être révisées afin de limiter l'utilisation personnelle d'Internet, de façon à ce qu'elle ne soit qu'accessoire ou occasionnelle, et le respect des politiques doit être surveillé. De façon générale, une grande majorité de l'utilisation d'Internet est d'ordre personnel.

Un échantillon aléatoire de 50 comptes utilisateurs a fait l'objet d'un examen approfondi pendant le mois de mai 2005. Pour ce groupe, le nombre de requêtes se situait dans une étendue allant de 44 220 requêtes (soit 2 106 requêtes par jour pour le plus gros compte utilisateur) à zéro requête pour le plus petit compte utilisateur. L'examen était fondé sur un échantillon statistiquement valide. Il a permis de constater que la proportion moyenne d'utilisation d'Internet à des fins personnelles de ce groupe était de 53 %.

Les cinquante plus gros comptes utilisateurs ont fait l'objet d'un examen approfondi pour le mois de mai 2005. Pour ce groupe, le nombre de requêtes se situait dans une très large étendue, allant de 2 098 002 (soit 99 905 requêtes par jour pour le plus gros compte utilisateur) à 29 761 requêtes (soit 1 417 requêtes par jour pour le plus petit compte utilisateur). Nous avons constaté que la proportion moyenne de leur utilisation d'Internet à des fins personnelles était de 66 %.

Le tableau ci-dessous présente un aperçu de l'utilisation d'Internet, comme l'a indiqué la Direction des services de technologie de l'information, pour le mois d'octobre 2005.

LES 100 SITES WEB AUTORISÉS LES PLUS VISITÉS EN OCTOBRE 2005
Selon la Direction des services de technologie de l'information

Catégorie (selon les STI)	Exemples	Pourcentage des 100 premières requêtes de sites Web	Pourcentage du trafic Internet total (oct. 2005)
Moteurs de recherche Internet	www.google.ca kh.google.com cdn.mapquest.com	41,7 %	25,9 %
Publicité	ad.doubleclick.net adcounter.theglobeandmail.com adme.411.ca	29,3 %	18,2 %
Sports, magasinage et divertissement	www.tsn.ca www.mls.ca	5,3 %	3,3 %
Actualités et médias	OttawaSun.com CBC.ca	4,2 %	2,6 %
Références	weatheroffice.ec.gc.ca www.Isuc.on.ca	2,4 %	1,5 %
Recherche d'emploi	Workopolis.com	2,0 %	1,3 %
Technologies de l'information	download.windowsupdate.com www.microsolft.com	1,6 %	1,0 %
Application de la Ville d'Ottawa	Interfleet.ca Library.Ottawa.on.ca	1,2 %	0,7 %
Autres	Comprend les sites « non classifiés »	12,2 %	7,6 %
Total		**99,9 %**	**62,1 %**

La Politique sur l'utilisation responsable de l'Internet prévoit des règlements et des directives sur l'utilisation appropriée d'Internet que doivent respecter tous les utilisateurs. Dans le cadre de notre vérification, nous avons constaté que la politique existante n'était pas respectée dans les domaines suivants :

- l'usage, s'il fait l'objet d'un examen public, n'est pas susceptible de mettre la Ville dans l'embarras ou de constituer pour elle une source de préoccupation;

- l'accès à partir des postes de travail de la Ville à des systèmes et à des comptes de courrier électronique auxquels la Ville ne souscrit pas (comme Hotmail) est strictement interdit;
- l'utilisation faite par tous les employés du réseau informatique et d'Internet fait l'objet d'une surveillance et d'un suivi;
- les utilisateurs ne doivent pas se servir de l'Internet à des fins illégales ou immorales;
- le partage de fichiers poste à poste;
- discussion sur le Web;
- services d'enchères par Internet;
- les comptes partagés;
- les annonces personnelles et les sites de rencontres; et
- les sites Web personnels.

Nous n'avons pas pu déterminer si l'utilisation d'Internet à des fins personnelles par les employés se faisait pendant les heures normales de travail. En effet, la Direction des services de technologie de l'information n'a pas fourni au Bureau du vérificateur général copie instantanée des dossiers.

L'utilisation personnelle du courriel n'était pas aussi importante que celle d'Internet. D'après un échantillon aléatoire de 50 utilisateurs, l'on a constaté que 16 % environ des courriels étaient d'ordre personnel. Tous les utilisateurs utilisaient le courriel pour une raison liée au minimum à un besoin d'affaires.

Une analyse des cinquante plus gros utilisateurs du courriel n'a pu être effectuée. En effet, les Services de technologie de l'information n'ont pas pu produire de rapport exact. Nous serions en droit d'attendre d'une organisation comme la Ville d'Ottawa qu'elle ait des outils éprouvés pour produire avec rapidité et exactitude des rapports sur des domaines tels les plus gros utilisateurs du courriel, les échantillons aléatoires d'utilisateurs, les messages envoyés et reçus et autres mesures connexes au courriel pouvant être utilisées pour l'analyse de l'utilisation de la messagerie électronique. Des méthodes de rechange pour suivre et surveiller les gros utilisateurs du courriel devraient exister.

La Politique sur l'utilisation responsable de l'Internet autorise expressément l'utilisation de cette ressource municipale à des fins personnelles. Bien qu'il soit raisonnable de s'attendre à une utilisation occasionnelle minimale d'Internet à des fins personnelles, nous pourrions nous attendre à ce que le degré d'utilisation d'Internet à ces fins soit similaire à nos attentes à l'égard des restrictions limitant l'utilisation personnelle du téléphone. La politique de la Ville sur l'utilisation du courriel n'autorise son utilisation à des fins personnelles que de façon accessoire, à l'instar des restrictions relatives à l'utilisation du téléphone. Puisque nous avons constaté une forte utilisation d'Internet à des fins personnelles, la Politique municipale sur l'utilisation responsable d'Internet doit être révisée afin de limiter l'utilisation personnelle d'Internet de façon qu'elle ne soit qu'accessoire ou occasionnelle.

Afin que les gestionnaires surveillent le personnel pour garantir que celui-ci utilise Internet et le courriel de façon appropriée, des rapports sur l'utilisation d'Internet et du courriel devront leur être fournis. Il incombe aux Services de technologie de l'information de surveiller et de contrôler l'utilisation d'Internet et du courriel. Cela doit inclure un processus de production de rapports sur les forts volumes et tendances d'utilisation inhabituelles, rapports devant être fournis aux gestionnaires afin que ceux-ci soient en mesure de déterminer si l'utilisation est appropriée.

À l'heure actuelle, les Services de TI ne fournissent pas aux gestionnaires de services des rapports réguliers sur l'utilisation d'Internet ou du courriel, pour que ceux-ci les examinent et s'assurent ainsi que

leur personnel utilise ces outils de façon appropriée. Cette surveillance peut être effectuée au moyen d'un processus visant à fournir des rapports à la direction en vue de ces examens.

Respect de la politique – Internet et courriel

Recommandation 18

Que les Services de technologie de l'information,

- **surveillent et contrôlent l'utilisation d'Internet et du courriel par les employés municipaux;**
- **élaborent des outils d'enregistrement appropriés pour fournir des rapports fiables sur l'utilisation du courriel;**
- **élaborent et mettent sur pied un processus permettant de fournir aux gestionnaires des rapports sur l'utilisation d'Internet et du courriel par leur personnel, de façon que la direction puisse déterminer si cette utilisation est appropriée;**
- **révisent l'Utilisation responsable des ordinateurs - politique municipales, afin de limiter l'utilisation d'Internet de façon qu'elle se fasse principalement à des fins professionnelles, et afin de limiter l'utilisation personnelle de façon qu'elle ne soit qu'accessoire ou occasionnelle.**

Réponse de la direction

La direction est d'accord avec ces recommandations.

Les Services de TI utilisent Websense pour surveiller et contrôler l'utilisation d'Internet au niveau global ou au niveau du système. Avant la vérification, les Services de TI ont lancé un vaste projet qui devrait être terminé pendant le premier trimestre de 2006. Ce projet vise à mettre Websense en œuvre de façon plus rigoureuse. Une vaste gamme de dispositifs de filtrage Websense supplémentaires a déjà été mise en place, ce qui améliore la surveillance de l'utilisation d'Internet et le blocage des sites Web non conformes au Code de conduite et à l'Utilisation responsable des ordinateurs - politique municipale. Les examens mensuels des rapports Websense par les Services de TI vont se poursuivre, ainsi que les modifications des catégories, le blocage des sites Web et les études complémentaires.

En 2006, les Services de TI vont améliorer la surveillance d'Internet à l'aide des outils de production de rapport Websense existants. Une analyse approfondie d'un minimum de 50 comptes Internet sera effectuée chaque semestre pour vérifier le respect de l'Utilisation responsable des ordinateurs - politique municipale. Les cas de non-respect seront examinés avec le concours des gestionnaires et de la section des Relations de travail de la Direction des services aux employés. Il est prévu que la mise sur pied de cet examen et ce suivi nécessitera de la part du personnel un travail équivalent à 1,5 ÉTP (2 700 heures).

Les Services de TI/Relations de travail contacteront les gestionnaires respectifs des 50 utilisateurs pris au hasard et des 50 plus gros utilisateurs examinés dans le cadre de la vérification. Les Services de TI, en collaboration avec les Relations de travail, fourniront le rapport de consultation d'Internet, ainsi que des lignes directrices sur la façon d'interpréter l'ensemble des données et d'approcher les employés à l'égard des préoccupations que pourrait soulever leur utilisation d'Internet.

Les Services de TI vont continuer de produire des rapports et des paramètres à l'aide de Promodag. Ils mettront également à l'étude des outils de surveillance et des capacités de production de rapports

supplémentaires pouvant permettre de surveiller les comptes de courrier électronique individuels. Les cas de non-respect de l'Utilisation responsable des ordinateurs - politique municipale seront examinés en collaboration avec les gestionnaires et les Relations de travail. À l'heure actuelle, l'effort supplémentaire à fournir pour effectuer ces examens et ce suivi n'est pas connu car il faudra attendre que les nouveaux outils soient identifiés et sélectionnés. Une pression budgétaire serait indiquée pour 2007, pour l'acquisition et la mise en œuvre de nouveaux outils de surveillance et de production de rapports.

La version révisée de l'Utilisation responsable des ordinateurs - politique municipale indique clairement que l'Internet et le courriel sont fournis pour « un usage professionnel justifié dans le cadre des fonctions assignées, mais peut également servir à des fins personnelles, à condition qu'il n'y ait pas d'abus », et que le non-respect entraînera des mesures disciplinaires pouvant aller jusqu'au renvoi. L'Utilisation responsable des ordinateurs - politique municipale sera révisée afin de garantir qu'elle s'applique de façon égale à l'utilisation d'Internet et à l'utilisation des courriels et tient compte de nos pratiques courantes.

Commentaires généraux de la direction

Les Services de technologie de l'information (STI) approuvent bon nombre des recommandations présentées par le vérificateur général. Là où la direction ne sons pas d'accord avec les constatations ou les recommandations présentées par le vérificateur général, une explication est fournie pour prouver le bien-fondé de cette position. Dans tous les cas, cela découle de recherches ou de consultations supplémentaires effectuées au niveau des fournisseurs, des experts en sécurité informatique et des meilleures pratiques de l'industrie.

Dans les cas où la direction a déjà entamé une action, une mise à jour de l'état de cette action a été fournie. Lorsque aucune action n'a été entreprise, le calendrier proposé, les incidences budgétaires et les résultats escomptés ont été identifiés.

1.6 Conclusion

Dans le cadre de cette vérification, la suffisance, l'efficacité et la fiabilité des mesures et des contrôles de sécurité en place à l'égard de l'utilisation d'Internet et du courriel ont été examinées, et la conformité de l'utilisation d'Internet et du courriel avec les politiques municipales a été évaluée. Bien que l'on ait constaté que les contrôles de sécurité actuellement en place sont généralement efficaces et fiables, des lacunes ont été identifiées au niveau de la suffisance de ces contrôles. La vérification incluait également un examen de la conformité de l'utilisation d'Internet et du courriel avec les énoncés de la politique actuelle. L'on a constaté que l'utilisation de ces outils à des fins personnelles est considérable. La Politique sur l'utilisation responsable de l'Internet et l'Utilisation responsable des ordinateurs - politique municipale devraient être révisées afin de limiter l'utilisation d'Internet de façon qu'elle se fasse principalement à des fins professionnelles, et afin de limiter l'utilisation personnelle de façon qu'elle ne soit qu'accessoire ou occasionnelle. Un programme visant à surveiller et à contrôler l'utilisation d'Internet et du courriel devrait également être établi.

Nous remercions la gestion pour la courtoisie et l'assistance qu'ils nous ont offertes pendant cette vérification.

1.0 Introduction

The Audit of Internet Usage and Controls was part of the 2005 audit plan brought forward by the City's Auditor General and received by City Council on December 15, 2004. This report documents the results of the audit findings including those controls and usage compliance components that were found to be functioning effectively and those that require remediation or implementation. The lifeblood of every organization is its information assets. For the City of Ottawa the vast amount of information assets is managed within Information Technology Services resources. The security of City assets must be protected with appropriate safeguards to ensure the continued confidence of both City constituents and staff. This audit is a review of the safeguarding of the City network from Internet threats.

2.0 Background

The use of the City's Internet and e-mail services are regulated and governed through two (2) policies. For the purpose of this audit, we reviewed the following policies, which were in effect at the time of our review:

- Responsible Computing Policy (August 13, 2001); and
- Responsible Use of the Internet Policy (December 11, 2003).

2.1 Internet Security Background

Proper control and protection of information assets is vital to City operations. In addition, the regulatory compliance implications and the public's level of trust expectations mean that the City must ensure appropriate information security management measures.

The basic building blocks of information security include the following properties:

- **Confidentiality**: information is made available or disclosed only to authorized individuals, entities, applications, or processes;
- **Integrity**: information consistency and authorized changes only; and
- **Availability**: information is readily accessible to its authorized users when needed.

It is broadly understood that an organization's required connectivity to the Internet brings substantial business benefits. However, it is also widely understood that continuously updated security measures must be implemented to reduce the risk of the Internet's ever evolving security threats to an organization's information and systems.

The Internet threats range from mild annoyances to harmful and destructive incidents. A failure to protect against these threats could include the following:

- Loss of critical information assets
- Loss of integrity of data
- Unwanted disclosure of confidential information
- Severed communications such as www.Ottawa.ca web site inaccessible from Internet or Internet bound e-mail failure

- Disruption of critical services
- Lost or delayed transactions

The consequences to the City could be:
- Damaged reputation
- Loss of public support
- Loss of staff faith
- Financial losses

2.2 Audit Scope

There are approximately 9,000 users of the Internet within the City of Ottawa. All users have access to e-mail, World Wide Web, and other Internet communications protocols such as MSN messenger chat for Ottawa Public Library users (on June 1, 2005, Instant Messaging was blocked for all staff excluding Ottawa Public Library), FTP, and specialized library catalogue systems protocols within the City of Ottawa. To facilitate this communication and transfer of information, the City's internal network has 220 high-speed wide-area network connections and 60 dial-up connections.

There are six ways the City network connects to the Internet:
1. Main Internet connection for public-facing Internet services such as Ottawa.ca, e-mail, and City & Library staff Internet usage;
2. Connection for Library public-use workstations;
3. Connection for OC Transpo public website;
4. ADSL connections for EFA public-use workstations;
5. ADSL connections using secure VPN tunneling between City facilities; and,
6. An isolated test connection for use in Information Technology Services lab environment.

Information Technology Services Branch reported a total of 26.7 million Internet "hits", performed by 6,226 users who accessed the Internet during the month of October 2005, which represents an average of 4,282 hits per user for that month.

The City's e-mail systems transfer over 200,000 e-mails daily.

The Ottawa Police Service was not included in the audit.

The audit included an investigation of a number of security controls within the City Internet infrastructure including the following:
- Internet firewalls
- Anti-Virus technology
- Anti-Spam technology
- Internet content filtering
- Key policies and procedures governing the use of, and the controls on Internet usage (for example, IM/IT Security Strategy, Responsible Use policies, Incident Investigation policies, Service Request policies).

The audit included an investigation of controls at the following sites using sampling techniques examining the Internet controls:
- 8 large City sites
- 6 small City sites
- The audit fieldwork was conducted during August and September 2005.

- The fieldwork included interviews with 23 City managers and staff for knowledge of policies and procedures.

In addition, the audit examined compliance of top users by volume and a random sample of users to the following policies using sampling techniques:

- Internet traffic (sites visited) for conformance to Responsible Use of the Internet Policy;
- Review e-mail usage for compliance to Responsible Computing Policy; and
- The sampling period for this audit was the month of May 2005 for Internet usage and the week of September 19 to 25, 2005 for e-mail usage.

3.0 Audit Objective

The audit objective is to provide an independent and objective assessment of:

- The adequacy, effectiveness and reliability of security strategy, policy, measures and controls in place over the usage of the Internet and e-mail; and
- Determine whether Internet and e-mail usage is compliant with the City policies.

4.0 Approach

Our approach to the audit was as follows:

- Review documentation collected (policies, protocols, procedures, and technical configuration documents affecting the management of Internet and e-mail);
- Conduct a Vulnerability Assessment against two City Internet sites or access points;
- Plan and conduct site visits and tests on 8 large sites and 6 small sites to both review the technical controls and also staff knowledge and practices of Internet and e-mail policies;
- Assess tools/mechanisms/logs used by managers to monitor and control processes;
- Review usage logs and compare to policy;
- Review staff Internet traffic to determine compliance to policy; and
- Review a sample of e-mail to determine policy compliance.

5.0 Acknowledgement

We wish to express our appreciation for the cooperation and assistance afforded the audit team by Management.

6.0 Observations, Findings, and Recommendations

6.1 Top “What is Working”

6.1.1 E-mail Dangerous Attachment Isolation

Positive impact on system/information confidentiality, integrity and availability.

This control quarantines inbound and outbound e-mail file attachments that are potentially dangerous. File types included in the quarantine list as those files that are typically executed by the Windows operating system. Examples of these attachments include traditional Windows executables (files end with extension of .exe) and other file types that may be business related but have the potential to contain malicious software. Heavy external e-mail usage users have observed a reduction of incoming e-mail with dangerous attachments. Users who required the

quarantined file attachments found the process to have the attachment released effective and efficient. The majority of the quarantined e-mails were deemed unnecessary and were deleted.

The findings were as follows:

- Anti-virus filtering correctly scanned and corrected attachments with viruses[1] including various archive formats.
- The quarantine feature correctly quarantined blocked file types.
- Restricted file types normally quarantined or blocked (such as .exe) could be bypassed by renaming the file attachments.

It was found that attachment filtering based on file name worked well. While it was not possible to bypass the anti-virus by renaming attachments, it was possible to bypass the restricted file types (such as .exe executable files) by renaming to allowed file types. Therefore, if a user wants to bypass this control, it is easy to do so.

Business Impact

This security control greatly reduces the City problems associated with e-mail propagated inappropriate information, malicious software attachments, and vulnerability exploitation, with results ranging from the embarrassment of inappropriate material found on systems, to disclosure of privacy information.

Savvy users cannot bypass anti-virus controls, however they can bypass file type blocking controls. Nonetheless the nine anti-virus engines will still block malicious file content.

Recommendation 1

That Information Technology Services investigate the tools used to perform blocking by file type to enable this feature regardless of extension.

See Management response with Recommendations 2 and 3.

6.1.2 Library and Employment Center Public Desktop Lockdown

Positive impact on system/information confidentiality, integrity and availability.

This control refers to the safeguards on personal computers that prevent non-privileged users from easily and quickly changing the configuration or adding software that causes these PCs to become attack vectors into the City network or the Internet, or result in theft of information. It is important to note that the computer network for the Ottawa Public Library patrons and the computer network for City staff share a common hardware platform on logically separate communication channels. Therefore, accidental or intentional configuration changes to the Ottawa Public Library patron PCs could, theoretically, provide a method and means to attack the City corporate network, exploiting any weaknesses in the logical segmentation of the City corporate network and the Ottawa Public Library patron network. However, during testing performed during this audit, the test cases used to attempt configuration changes on these systems failed to effect changes to the systems (see below).

[1] EICAR test virus used for all virus testing. EICAR is a benign string that triggers anti-virus controls to enable safe testing of anti-virus systems.

The findings were as follows:

- The anti-virus system detected files infected with the EICAR virus on attempts to write the file to disk.
- The anti-virus did not detect a read of a file infected with the EICAR virus.
- The anti-virus did not detect the execution of the EICAR virus.
- The anti-virus pattern file was found to be up to date.
- It was not possible to modify key system files to change the operation or configuration of the system.
- It was not possible to change the IP routing on the system (which could be used to attack the network).
- The Bajai content filtering software was found to prevent access to common blocked sites. The Bajeye content filtering also functioned to block offensive images in most cases.

The anti-virus system on these systems did detect the test virus when attempting to write a virus to disk, however it failed to detect the virus on read or execute. This configuration error could allow a virus to attack the network if executed from an e-mail or Internet download or from removable storage.

Various attempts were made to change the configuration of these systems. The configuration lockdown proved effective against the attacks. The same controls also prevent a malicious hacker posing as a patron to either capture confidential information from other patrons or as an attack vector against other hosts on the Internet.

The Bajai content filtering system prevents access sites on the blocked policy list. In addition, the Bajeye filtering tool prevented the loading of images that met the blocking criteria. However, like all current blocking tools, it does not cover all web sites on the Internet nor all images (e.g. tanned skin could cause the Bajeye filter to fail).

The system developed on Deep Freeze technology provides effective system lockdown and simple reboot quick recovery. It includes a regularly updated Symantec Antivirus, in addition to a regularly updated centralized and distributed (respectively) Bajeye web filtering.

Business Impact

This security service greatly reduces patron misuse of City public resources, while providing them a heightened level of protection against inappropriate material, malicious software and Internet abuses. It also significantly reduces the program's information technology support costs. However, providing an automated Windows XP patching, and the latest Symantec Antivirus version, incorporating additional malicious software protection, would greatly improve library and employment centre patron protection.

Recommendation 2

That Information Technology Services deploy the latest Symantec Antivirus version.

Recommendation 3

That Information Technology Services update the configuration of the Antivirus systems to include anti-virus checking on read from disk and before program execution.

Management Response

Management agrees with recommendations 1, 2 and 3.

IT Services is investigating a new feature recently available for the first layer of virus-scanning protection, which permits blocking of file types regardless of the extension used. Testing to ensure there is no negative impact on e-mail delivery services will occur in Q1 2006.

IT Services considers that the risk of using the current version of Symantec Antivirus (7.61) is mitigated as three additional layers of anti-virus and malicious file protection also safeguard the City network, and Symantec continues to issue updated virus signature files per the support agreement up to January 31, 2006.

It is not uncommon for an organization of the size of the City of Ottawa to delay or skip version upgrades of software products. Upgrades are done either because the new functionality offered is needed by the City and is supported by a business case for the upgrade, or because the product is no longer supported by the vendor. IT Services has evaluated the additional features and business case for each new version as it is released. In fact, the City partnered with Symantec in Q1 2005 to beta-test version 10, as this is the first version to add features to safeguard against the current threat from spyware. Following this evaluation, Symantec recommended in late Q3 2005 that the City begin a managed upgrade directly from version 7.61 to Symantec Antivirus version 10.

IT Services initiated the upgrade to Symantec Antivirus 10 in Q4 2005, to be completed by January 31, 2006. This upgrade includes an assessment of the productivity impact of including anti-virus checking on read from disk and before program execution.

6.1.3 E-mail SPAM

Positive impact on system/information integrity and availability.

While there is great debate about a conclusive definition for SPAM, it can be loosely defined as follows;

> *A simple definition of spam is unsolicited e-mail messages, generally commercial or promotional in nature, usually sent in bulk. The key word here is unsolicited.*
>
> *Most spam messages are commercial advertisements for products or services, but many non-commercial messages can also be considered spam, such as: promotional messages, political messages, press releases, charitable solicitations, scams and "get rich quick" schemes, jokes, chain letters, hoax messages that advise the recipient to forward the message to all entries in their address book.*[2]

The findings were as follows:

[2]The Open Group, http://www.opengroup.org/messaging/public/apr-2003/spam_call_to_action.htm#what%20is%20spam

- Based on responses from user questionnaires that asked if users were receiving SPAM, all users reported dramatic reductions in SPAM since the introduction of the SPAM filtering tools.
- High volume Internet and e-mail users reported a small amount of SPAM continues to penetrate the e-mail system (about 1% per day for e-mail users receiving 100 or more e-mails per day).
- While there is a SPAM e-mailbox for users to send any SPAM e-mail that penetrates the SPAM filters for analysis, none of the users interviewed during the site visits recalled its existence. It should be noted that the sample size consisted of 23 staff and managers. In addition, some of the users interviewed received less than 1 SPAM e-mail per month and are perhaps not inclined to report these e-mails.
- The SPAM e-mailbox has been monitored daily since 2003. Since the implementation of the anti-spam firewall in January 2004, samples of recurring spam have been submitted to the anti-spam vendor for inclusion in the spam filtering rulebase. The spam e-mailbox and firewall are also regularly monitored for emergent virus, worm, and "phishing" threats. Trends are monitored and reported on monthly to the Chief Information Officer.

Users have observed a significant reduction in e-mail SPAM. There are still SPAM e-mails being received by high volume e-mail users however, these e-mails are a more targeted type of e-mail that does not meet the technical match criteria currently used by the City's SPAM filters. This does not represent a failure of the current SPAM system used by the City but rather is a result of more sophisticated SPAM e-mails designed to bypass the current technology. Regardless, all users reported a dramatic reduction in the volume of SPAM e-mail received which is supported by the system reports identifying substantial volumes of e-mail being blocked.

Business Impact

This has significantly reduced the amount of SPAM e-mail that City staff must process and, reduced the possibility of the SPAM setting off a malicious software infestation, and reduced the e-mail delivery system resource requirements.

Recommendation 4

That Information Technology Services:

- **Review the level of awareness of the SPAM e-mailbox and increase visibility if warranted; and**
- **Continue monitoring the effectiveness of the current SPAM filtering tool.**

Management Response

Management agrees with these recommendations.

The spam@ottawa.ca mailbox continues to be part of IT Services' ongoing security awareness program. Over 1,000 e-mails received by City staff from external sources are submitted monthly to the SPAM mailbox for review. In addition, four City Brief articles were published in 2005 on the topic of SPAM, each including a reminder about the availability of the SPAM mailbox. IT Services will continue to remind staff of the SPAM e-mailbox regularly.

Upgrades to the SPAM filtering service are implemented by IT Services when available from the vendor, to ensure continued effectiveness of the service. As noted in the report,

monitoring of the SPAM filtering service is performed daily, and reviewed monthly by IT Services.

October data from MessageLabs indicated that 65% of all e-mail worldwide was identified as SPAM. Of the 50,000 e-mails received from external sources daily to the City's 9,000 e-mail users, slightly over 50% is identified as SPAM and immediately rejected. Roughly 0.5% of these e-mails are SPAM that is not identified or rejected, and successfully reaches a City recipient – 250 e-mails per day for the entire City. Users are encouraged to forward SPAM messages to IT Services to assist in increasing the effectiveness of the SPAM filtering service.

6.1.4 HTTP Web Site Filtering

Positive impact on system/information confidentiality, integrity and availability.

The City has implemented a number of different controls to enforce the Responsible Use of the Internet Policy. In addition, this service also supports the protection of the City network from sites known to include malicious software. This section discussed the control of the most prevalent form of Internet use, the HTTP protocol common to most web sites. It excludes all other protocols (including the HTTPS protocol common to online banking and purchasing sites), but HTTP is the dominant protocol for transferring data from web sites. Notwithstanding some implementation issues that could minimize this control, the Websense and Bajeye http web site filtering is working well at implementing Responsible Use of the Internet Policy controls.

The findings were as follows:

- The Websense content filtering tool worked to block a wide range of productivity impacting and prohibited sites as defined in the Responsible Use of the Internet Policy.
- Websense content blocking of the Premium Security group sites (sites known to contain malicious code are included in this Premium Group) was not tested, but should be effective in preventing users from browsing sites that are known to contain malicious software thus protecting the City network.
- Websense was not universally implemented for all users within the City network. In particular, the Ottawa Public Library staff are a general exception to this standard, as per the Ottawa Public Library Board Policy.
- A handful of hosts (servers or workstations) were found exempt from the HTTP content filtering.
- Four workstations at the Don Gamble Complex were found to be exempt from Websense filtering.
- A computer savvy user can use various methods to bypass the Websense controls.

Testing of the control verified that standard request for websites on the banned lists is correctly blocked. However, further testing showed that it is possible to bypass the intent of the controls through various methods such as proxy servers, remote control servers, and specific bypasses such as viewing images that would otherwise be blocked through images.google.com.

The Ottawa Public Library Board Policy regarding Internet usage for staff is guided by their intellectual freedom standards. This freedom that Ottawa Public Library staff enjoy includes unfiltered web site access and services such as webmail and instant messaging.

Finally, this control blocks access to a specific Websense category that includes sites known to contain malicious code. However, since all Library staff are exempt from this filtering, the risk to the Library systems and the whole internal City network is increased as they are interconnected. There is no separation or additional controls between the Library staff and the rest of the City network. Thus, the controls in place prevent users on the City network from visiting a web site known to contain malicious software, which can be visited by an Ottawa Public Library user. An exploited Library system could go on to propagate malicious software or be leveraged to leak information from any part of the City's network.

Business Impact

This security control greatly reduces the risk of Internet inappropriate material exposure to City staff by blocking access to these sites. In addition, further sites including some webmail sites are blocked leading to a reduced misuse of time spent "surfing" for non-business reasons.

This service further limits staff exposure to numerous web sites which contain malicious software and system vulnerability exploitation code which would be unknowing or misleadingly installed, leading to potential information disclosure or system unavailability.

A minimum level of Library filtering should be put in place to protect the City's network. If staff from the Ottawa Public Library continue to be bound by separate policies for use of the Internet (in particular allowing unfiltered access, access to external e-mail systems, and access to unauthorized applications using the Internet such as peer-to-peer), then Information Technology Services should consider separating the unfiltered Ottawa Public Library staff from the rest of the City network via key safeguards such as firewalls and other security systems. (Note: this model is already used with the Ottawa Police network).

Recommendation 5

That Information Technology Services:

- **Tighten the Websense service implementation to reduce possibility of service bypass.**

Management Response

Management agrees with this recommendation.

In 2005, prior to the audit, IT Services launched an extensive project to enhance the rigour of the Websense implementation, scheduled for completion in Q1 2006. At the time of writing this response (November 2005), an extensive range of additional Websense filtering features is now in place.

The audit findings identified one small site (the Don Gamble Community Centre) that allowed City of Ottawa staff unfiltered access to the Internet. This was a subnet routing issue that misidentified these four City staff to Websense as Library staff workstations, which are unfiltered (see below). IT Services has corrected this routing issue.

- **Review some level of Library filtering to reduce the risk, such as a limited number of isolated general use systems for unfiltered web access. If this cannot be completed to an appropriate level, then Information Technology Services should consider separating the Ottawa Public Library from the City's system.**

Unfiltered Internet access is provided to Ottawa Public Library (OPL) staff for reasons of intellectual freedom. This is as a result of a Library Board directive and therefore is a governance issue with the Library Board and outside the jurisdiction of the IT Services Branch.

Since 2001, a considerable amount of effort from IT Services has been directed to manage the risk of this configuration. For example, Library workstations are on separate network segments that make it easy to isolate viruses, worms and spyware in the event of a malicious code outbreak. On the advice of IT Services staff, Library Management agreed, in October 2005, to allow IT Services to protect their workstations from Internet-borne malicious code. The workstations used by Library staff do not allow staff to visit malicious websites, however they remain completely unfiltered for all other website content.

Given the OPL is governed by the Library Board, it may not be possible to influence the Board to reverse the decision to allow unlimited access to Internet sites based on the principle of intellectual freedom. Therefore if filtering cannot be implemented to a reasonable level, ITS Branch agrees with the recommendation that consideration should be given to separate the Ottawa Public Library from the City's system. This would be a significant undertaking as the Ottawa Public Library (OPL) is spread across 33 different sites throughout the City. Furthermore, separating the Ottawa Public Library from the City of Ottawa network would incur significant additional costs, due to the sharing of business applications and IT Services resources between OPL and the City.

It is estimated that the cost to separate the Ottawa Public Library from the City's network would be $30,000 of one time capital funding and $150,000 of annual operating costs, including the funding of 1 additional FTE (or equivalent). A budget pressure will be identified for the 2007 budget.

6.1.5 Desktop/Laptop Enterprise Anti-virus

Positive impact on City system/information confidentiality, integrity and availability.

Anti-virus on the City system is enforced at up to three layers within the network. Within the network, the desktop PCs and servers are protected by Symantec Antivirus; Microsoft Exchange (the e-mail server) (running Antigen which uses seven unique parallel anti-virus scanning engines), and the SPAM filter solution (running Kaspersky Anti-Virus). Therefore, e-mail may be scanned by up to three independent anti-virus systems using nine unique virus-scanning engines. Other communications such as web-based browsing are filtered by the desktop anti-virus solution and the Websense filtering software. With a small exception, City systems had corporate Symantec Antivirus running with up-to-date virus signatures.

The findings were as follows:

- The signature files on all anti-virus systems were found to be up to date.
- Anti-virus was found deployed on nearly all workstations and servers inspected.
- The configuration of the Symantec Antivirus on the desktop was found to not scan files on read or on program execution for viruses.
- The Symantec Antivirus is several versions out of date and no longer officially supported and lacks some of the new security features available in later versions.

Testing of the anti-virus systems showed that the EICAR test virus was detected correctly when written to disk, however, the configuration did allow read of files and execution of files without correct scanning. This configuration introduces vulnerability in the anti-virus posture of the City. The configuration of anti-virus systems needs to be examined to provide broader coverage of detection of virus events before they can be executed. It was found that it is possible to execute programs containing virus (a benign test virus) of City systems. While the particular configuration vulnerability weakness limits exposure, it must be investigated and remedial actions performed.

The current version of Symantec Antivirus was found to be several versions out of date and no longer fully supported. According to the Symantec documentation, they will only provide a best effort phone support. There will be no code corrections provided on the current version that the City uses. There is a small risk that the Symantec software may not operate in the City's environment due to configuration or program changes and Symantec will not provide a fix for that environment.

The City is an active beta tester of the latest version of the Symantec Antivirus. Based on the recommendation of Symantec, who assessed the functionality improvements between version 7 and version 9 as minimal and given the current threat environment, the City agreed to work with Symantec to pilot test a beta version of version 10 prior to conducting a managed upgrade in Q4 2005. Version 10 is the first Symantec product to address the ever-increasing Spyware problem. The City has evaluated and accepted the current risk noted above. Reducing this risk is a support contract that the City of Ottawa maintains from Sensible Security Solutions to provide 24x7 support for all anti-virus products used by the City, including those provided by Symantec, and services in defense of any malicious code outbreaks. Finally, anti-virus definitions continue to be released for the current anti-virus client; and, targeted desktop anti-spyware cleanup tools are used by the Service Desk.

Adoption of the latest version of Symantec will increase the coverage of anti-spyware controls on the City network. As with the improvement multiple anti-virus scanning engines provide, multiple spyware vendors will provide greater depth of coverage preventing spyware code.

Business Impact

This essential security service severely restricts the effects of a virus infestation to an individual system and via ripple effect, the network as a whole. This includes system unavailability, and modified, lost or leaked information.

However, the client version is now three major revisions old and is no longer officially supported, restricting its functionality and support. In addition, this particular version does not incorporate the expanded threat detection capabilities of the latest version. While the City does

have a layer of malicious website blocking from Websense, the latest Symantec Antivirus software adds an additional layer of protection against spyware threats – a key emerging attack vector.

Recommendation 6

That Information Technology Services:

- **Deploy the latest Symantec Antivirus version; and**
- **Update the configuration of the Anti-Virus systems includes anti-virus checking before file read and before program execution.**

Management Response

Management agrees with this recommendation.

IT Services considers that the risk of using the current version of Symantec Antivirus (7.61) is mitigated as three additional layers of anti-virus and malicious file protection also safeguard the City network, and Symantec continues to issue updated virus signature files per the support agreement up to January 31, 2006.

It is not uncommon for an organization of the size of the City of Ottawa to delay or skip version upgrades of software products. Upgrades are done either because the new functionality offered is needed by the City and is supported by a business case for the upgrade, or because the product is no longer supported by the vendor. IT Services has evaluated the additional features and business case for each new version as it is released. In fact, the City partnered with Symantec in Q1 2005 to beta-test version 10, as this is the first version to add features to safeguard against the current threat from spyware. Following this evaluation, Symantec recommended in late Q3 2005 that the City begin a managed upgrade directly from version 7.61 to Symantec Antivirus version 10.

IT Services initiated the upgrade to Symantec Antivirus 10 in Q4 2005, to be completed by January 31, 2006. This upgrade includes an assessment of the productivity impact of including anti-virus checking on read from disk and before program execution.

6.2 Top Challenges

6.2.1 HIGH Priority - Logging and Device Monitoring

Negative impact on system/information confidentiality, integrity and availability.

System log files contain essential information about the operational health and also about security events. Examples of log information include authentication events (e.g. failed logins), changes to configuration, and reboots as well as information about traffic and data events. The collection and review of this data is critical to understanding “normal” patterns and detecting deviation from “normal” patterns can indicate potential operational health or security events. In addition, device status needs to be monitored in near “real time” to ensure that the device status is known and that there are timely alerts to significant operational events.

The findings were as follows:

- Device logging was found to be limited on some devices and non-existent on one key security device.
- Logged event timestamps are suspect given that the clocks on the key devices are not centrally synchronized – one clock was observed to be around five hours off.
- Logging analysis, when performed, is manually intensive.
- Device logging analysis was found to be ad hoc for a number of devices.
- The PIX firewalls are reachable via the telnet management protocol from anywhere within the City network.

The PIX firewalls were found to be logging at level 4. This level was selected due to a need to minimize the amount of log data generated. However, level 4 logging excludes the recording of certain events such as failed or successful logins or configuration changes, both of which are critical to identifying attempted or successful compromise of these systems. One firewall was found to be logging to the console only – this has a very limited memory and is overwritten when the buffer fills. Given that the firewall is reachable from an IP address on the City's corporate network, attempts to use a brute force attack on the firewall password and other potential attacks must be monitored. A record of when changes have been made to the firewall must also be tracked. This allows correlation of modifications to the firewall configuration to change requests submitted.

Correlation and temporal sequencing of events is critical to incident investigation. It was found that the system times on the PIX firewalls was set manually and not automatically synchronized with a central time server. One firewall was found to be 5 hours off the current time. These inconsistent times would make incident investigation difficult or impossible. The corporate servers investigated were found to be configured to synchronize their times with a central timeserver.

Logging analysis, when performed, is manually intensive. A review of the logs from the PIX firewalls required manual manipulation of large numbers of log files. Information Technology Services only review firewall log files when a suspected event has occurred. Review of firewall log files is not performed proactively to identify events or establish baselines for various system parameters. Log review of anti-virus events was found to be effective but given that it is a manual activity, is only performed during regular daytime business hours, and is subject to human error.

There was little monitoring of the reliability of the some services. The Websense HTTP filtering system consists of the corporate firewall for the enforcement and the Websense server for the database and validation service. A review of the log files from the firewall indicated a small number of consistent failures of this system to function properly. The firewall failed to properly validate user requests to access web sites. The level of failures was not significant – less than 1000 URL looks up requests per day failed: these failures were due to a too busy server or Websense was offline for maintenance. However, there was no evidence that Information Technology Services are periodically monitoring to determine the reliability of the service. Trend analysis of the reliability of services that fail open is required to detect failure levels.

The key corporate firewalls are operating in a redundant mode. However, monitoring of these systems for the operational health of the primary and secondary devices was found to be ad hoc. It is possible and probable that the failure of the primary PIX firewall at any of these locations would remain unnoticed. There is evidence in the logs that this may have been the case during early 2004. Essentially, failure of the primary PIX firewalls would go undetected resulting in potential complete failure should the secondary firewall fail.

Finally, given the large volume of log data, automated tools to assist review of not just individual system logs, but also a system wide view of the log data for correlated analysis. A centralized log repository and analysis tools will provide analysts with all relevant log information for investigation. Correlation of multiple events on individual systems and correlation of events on different systems can help identify threats.

Business Impact

The limited logging and monitoring of key security network points means that enforcement control effectiveness cannot be properly measured. Events ranging from the access to the web based public registration service, to successful or attempted breach of confidentiality of client privacy information from an automated credit card payment system or other sensitive data could occur without timely detection. Timely detection will help the City respond proactively to such threats.

A limited 3-month retention of logging information further severely hampers any security incident investigation or control auditing.

In addition, centralized log analysis can help reduce the effort required by IT Security to analyze log events from multiple systems for correlation.

Recommendation 7

That Information Technology Services:

- **Review logging and monitoring processes and systems for effective operational system health and policy enforcement monitoring;**
- **Identify log events that require "real time" detection and alerting and implement appropriate processes;**
- **Review all security devices to ensure appropriate logging coverage;**
- **Ensure all device clocks are centrally synchronized for effective event correlation;**
- **Review regulatory and City policy requirements for an appropriate logging data retention period;**
- **Consider feeding log and monitoring data into a Security Information Management (SIM) tool for automated event analysis and correlation, to better provide a near real time City security posture;**
- **Ensure all devices are logging operational health and security events as a minimum; and**
- **Enable system logging on all devices.**

Management Response

Management does not completely agree with these recommendations.

Industry best practices do not support full logging on all devices at all times due to the high cost. IT Services implements additional logging and alerting on a selective basis, such as with certain high-risk devices or where there is a concern with a particular device.

As part of the Enterprise Security Review project initiated in Q1 2005, IT Services has contracted a third party security company to perform a detailed review of logging and monitoring processes and systems, including an assessment of the cost impact of these recommendations. The review will be completed in Q1 2006. If additional logging is required, a budget pressure will be identified in the 2007 budget. IT Services has implemented alerting for device failure on all servers and network devices.

IT Services has updated all firewalls to receive a synchronized time from NRC.

A review of regulatory and City policy requirements for logging data will be completed in Q2 2006, following the detailed review of logging and monitoring processes and systems in Q1 2006. Log data will be retained in accordance with the City's Records Management Policy and By-Law.

The need for additional logging and Security Information Management (SIM) tool will be assessed in Q2 2006 and if required a budget pressure will be identified in the 2007 budget. Additional logging is estimated to cost between $75,000-$150,000. To purchase and implement a SIM is $150,000, with ongoing operating costs in excess of $200,000 per year. Ongoing FTE (or equivalent) requirements are unknown at this time.

6.2.2 MEDIUM Priority - Change Management

Negative impact on system/information confidentiality, integrity and availability.

The process/system for tracking and auditing enforcement system, architecture and policy implementation changes – although a formal process – is not consistently followed. In many cases, change documentation was missing or incomplete. A formal repeatable change management process is necessary for effective multidiscipline team coordination. It also provides the foundation of disaster recovery and incident response management.

The finding was as follows:

- Change requests could not be produced for a selection of inbound rules on the firewall.

Currently, it is not possible to track firewall rules to the rule requestor. Periodic reviews of rules on firewalls should be conducted, however, given that rules are not tracked to requesters, it would be difficult for the City to perform this task, thus it is possible that rules exist on the firewall for which there is no current requirement.

Business Impact

A solid Change Management process/system provides a mechanism to ensure only authorized security control openings in the City's defensive posture. The authorization process is based on proper risk management to ensure the appropriate City security controls for regulatory

compliance and the demands of its citizens. Should a system fail, or a security breach occur, complete Change Management records would help ensure fast, effective recovery with minimal loss of information or disruption. It will also provide a basis to analyze the breach to determine if control readjustment could be instituted to prevent a reoccurrence.

Recommendation 8

That Information Technology Services:

- **Implement a more robust Change Management process/system within Corporate Services; and**
- **Enforce the formal Change Management process for all changes to the firewalls and other security systems.**

Management Response

Management agrees with these recommendations.

The current Change Management process in place since 2001 was enhanced in Q4 2005 to encompass all IT Services divisions and the requirement to comply with the City's Records Management Policy.

The Chief Information Officer reminded all IT Services Managers and Program Managers in November 2005, of the requirement to adhere to this Change Management process. This includes the requirement to document results achieved and record these centrally using the City's Records Management framework.

6.2.3 MEDIUM Priority - IT Security Policy, Policy Interpretation, and Policy Application

Negative impact on system/information confidentiality, integrity and availability.

A review of the IT Security policies, the interpretation of the policies, and the application of those policies was conducted. The policies ensure that authority for IT security is assigned, management intent for IT Security is defined, and consistent interpretation of the need for IT security is applied by the practitioners within the organization.

The findings were as follows:

- Not all users and systems were bound by the Security policy. In particular the Ottawa Public Library staff were exempt from key policy directives designed to protect the network.
- The IT Security policies do not prohibit the use of non-City systems for processing City data.
- The IT Security policy does not explicitly prohibit the installation of unauthorized software. This, combined with the large number of users who have administrator rights on their system, allows users to install software such as SKYPE (a VOIP software) and Limewire (a Gnuttella P2P software), and other software that may introduce malicious software, spyware, or introduce other IT support problems on the network.
- There was no cryptographic policy despite the guidance of using such software in the IT Security Policy for e-mails with sensitive content.
- A large number of users (~1500) were found to have administrator rights to their local workstation giving them the ability to install software or change the configuration.

Of concern was the incomplete application of key components of the Responsible Use of the Internet Policy. In particular, the Ottawa Public Library staff are exempted from all Internet content filtering (for HTTP web sites). It is important to recall that the City network is linked together on a common network infrastructure with homogeneous PCs and common infrastructure. All major City departments and the Ottawa Public Library services share the network and IT Systems on that network without separation by security controls. This City network is protected at the perimeter through various controls mandated through policy. One of these key controls protecting the perimeter is the prevention of City employees from accessing certain web sites known to contain malicious code. The intent of these sites is to cause an "infection" of the computers that connect to these sites – these computers are the City PCs. To protect against this threat, users and the City network must be prevented from other City users traveling to these sites. The Ottawa Public Library staff are currently exempt from the content filtering policy that prevents access to these malicious sites. Ottawa Public Library staff could navigate or be linked to these sites and cause "infection" of the whole City network. While recognizing that the Ottawa Public Library staff need access to a broad range of sites for academic purposes, access to sites that exist purely for the purpose of propagating malicious software should be prevented.

Some policy gaps were observed, including the absence of a policy on use of non-City controlled desktops/laptops for City network access and information processing, and a cryptographic policy.

There are two key considerations that do not appear to address the alignment of services with security of those services:

- Security services should have the same SLA as the business service it is protecting.
- Security service should fail open ONLY when there is an overwhelming need for the service to operate despite the failure of the security service.

Several instances of non-standard PC software were found while investigating traffic on the network. In particular, the VoIP software SKYPE and the P2P software Limewire was found installed on some PCs. Both of these software were installed for personal use, yet consume system resources and potentially cause reduced PC productivity through system impact and other negative system impacts.

The large number of users with administrator rights on their local workstations introduces security vulnerabilities. Users with administrator rights can install software. Evidence was found of unauthorized software on workstations that could introduce malicious code (unreliable source for these applications), could cause system performance problems (unstable program code due to design and development standards not robust), and could cause a negative impact to the network.

It is recognized that a large percentage of these users require administrator privileges to configure laptops to suit the different operating environments. Information Technology Services should review alternate methods to allow the minimum required level of configuration and software access.

Interviews of employees during the site visits, both new and longer-term employees had security policy awareness that ranged from cursory to complacent. Most leveraged the attitude "if I can't do it, then I am not allowed".

Business Impact

Clearly defined policies lead to better interpretation and application of these policies across a multi-disciplined team. Combined they lead to a highly level of system and information security. Without them, systems become vulnerable to attack and information confidentiality is at risk.

Effective policies require a means to measure their implementation, especially if the policy has a possible effect on resource allocation. The policy's implementation and monitoring mechanisms are the responsibility of Information Technology Services.

Recommendation 9

That Information Technology Services ensure the policy prohibit the installation of software not officially sanctioned.

Management Response

Management agrees with this recommendation.

Section 6.4 of the revised Responsible Computing Policy, approved by City Management in September 2005, states: "Users shall not install or download software, shareware, freeware or any other application program onto City-owned IT assets without the express written permission of ITS."

Recommendation 10

That Information Technology Services ensure the policy prohibit the use of non-City approved computing resources for processing City data and assets.

Management Response

Management does not completely agree with this recommendation.

This recommendation applies to the following two situations:

- Use of non-City hardware by staff and/or consultants on the City network (e.g., laptops). Processing City data and assets using non-City hardware (e.g., home computers). IT Services concurs with the recommendation with respect to the use of non-City hardware on the City network (e.g., laptops). In section 6.3 of the revised Responsible Computing Policy, approved by City Management in September 2005, the Policy states: "Non-City hardware shall not be connected to the Corporate network without the express written consent of the ITS Branch."

- IT Services does not agree with this recommendation with respect to processing City data and assets using non-City hardware (e.g., home computers). Such a restriction would prohibit the use of web-mail from a home computer, or working from home on a Word document or Excel spreadsheet. The Responsible Computing Policy clearly

defines employee obligations to safeguard electronic and information records in their custody, whether being processed at a City facility or not. The City's Defence-in-Depth Strategy (see section 7.2.4 C) mitigates the risk to the corporation from malicious software brought from a non-City computing environment.

Recommendation 11

That Information Technology Services review the retention periods for e-mail (including deleted e-mail) and compare to use of this data as corporate records and industry best practices.

Management Response

Management agrees with this recommendation.

The retention period for e-mail was reviewed against federal, provincial, and municipal legislation prior to approval of the Records Retention and Disposition By-law approved by Council and the Records Management Policy in 2003. Automated retention rules for e-mail were implemented as a part of an upgrade to the Exchange Server product in September 2005, to ensure compliance with this by-law and policy.

Recommendation 12

That Information Technology Services review the users with administrator rights on their workstations, and where not justified and required, remove the administrator privileges for that user.

Management Response

Management agrees with this recommendation.

A rigorous documented formal process is followed whenever any user requires local administrative rights.

As part of the Enterprise Security Review project, a review will be conducted regarding administrative access rights for IT Services with recommendations provided to the IT Services Management team in Q1 2006. This review will be repeated on an annual basis.

More restrictive administrative rights for laptop users are being implemented as part of the life cycle laptop replacement program. At this point, funding is available to replace roughly 100 units of the total fleet of 900.

Roughly 50% of the current fleet of City laptops are now running a version of the operating system that offers administrative rights control. IT Services plans to implement these administrative rights restrictions by the end of Q1 2006. The remaining 50% of the City laptop fleet needs to be replaced.

Funding of $700,000 and one (1) additional FTE (or equivalent) will be required in order to accelerate this replacement program to be completed over twelve (12) months. A budget pressure will be identified for the 2007 budget to accelerate this replacement program to be completed over twelve (12) months.

6.2.4 MEDIUM Priority - IT Security Delivery Roles

Negative impact on system/information confidentiality, integrity and availability.

The role and authority of IT Security must be clear to all City staff for the group to function effectively.

The following roles and responsibilities were not clearly defined:

- IT Security desires that all Internet access be monitored using Websense; currently, some firewall rules still exist which bypass this monitoring.

Filtering exclusions are implemented on both the CISCO PIX (operational, policy implementation and monitoring control - TI) and Websense servers (system control – server group, application control – TI and policy control – TI & IT Security). IT Security would like to see all the exception definitions removed from the PIX and defined on Websense so that all activity could be logged. This activity has been ongoing through 2005 during the joint reengineering of the Websense product between TI and IT Security.

Regarding the specific issue noted above, Websense should be used to monitor all Internet traffic.

Business Impact

Clearly defined policy implementation authority and roles lead to better enforcement and auditing the security policies across a multi-disciplined team. Clear delimitation leads to a highly level of system and information security. Without them, systems become vulnerable to attack and information confidentiality is at risk.

Recommendation 13

That Information Technology Services:

- **Review organization roles and responsibilities with accompanying agreements, such as SLAs; and**
- **Clearly define roles/responsibilities and define processes to ensure control implementation and monitoring is covered.**

Management Response

Management disagrees with these recommendations.

IT Services has reviewed existing organizational roles and responsibilities, and believes that these roles and responsibilities are clearly delineated and effective. Separation of duties and other organizational control mechanisms are fully implemented and maintained across the entire branch.

6.2.5 MEDIUM Priority - Encryption Policy

Negative impact on system/information confidentiality, integrity and availability.

An encryption policy is required to identify both the minimum strength of encryption and define under what circumstances encryption should be applied. In addition, key management should be defined. This encryption policy should be applied to both data communications and data storage. However, the scope of this audit applies only to data communication.

Internet communication using weak encryption was found connecting DC4 to an Ottawa Public Library test system. The communication terminated on the PIX firewall at DC4 and a firewall located in the 100 Constellation library test lab. Internet communication is via an Allstream (AT&T) Internet circuit. This weak encryption could result in confidential information being exposed to unauthorized entities.

In addition, the City's Responsible Computing Policy identifies that encryption should be used for the transmission of sensitive e-mail content. Yet, there appears to be no policy or approved tools for this control.

Business Impact

Possible compromise of either the applications or systems located at this site. This weakness could result in exposure of compromised data, or exploitation of the systems protected by the encrypted communications tunnel.

Recommendation 14

That Information Technology Services develop an Encryption Policy to address key aspects of encryption related to the City's operations and requirements.

Management Response

Management agrees with this recommendation.

Encryption technologies are currently used to safeguard specific systems, but these *de facto* standards are not presently in one reference document. Existing encryption standards will be collected and documented by Q2 2006.

Recommendation 15

That Information Technology Services identify tools for encryption of sensitive e-mail content.

Management Response

Management disagrees with this recommendation.

The revised Responsible Computing Policy, section 7.1, as approved by City management in September 2005 stipulates that sensitive information is not to be transmitted via the corporate e-mail system.

An enterprise wide e-mail encryption solution would be for internal use only and would not necessarily be compatible with external partners, as there is no national or international standard for e-mail encryption.

Should an enterprise-wide e-mail encryption solution be required, it is estimated to cost $100,000 and require 2 FTEs (or equivalent) to administer. A budget pressure would be identified for the 2007 budget.

Recommendation 16

That Information Technology Services implement strong encryption on the link between DC2 and the library lab network that uses the Internet for communication.

Management Response

Management agrees with this recommendation.

IT Security will investigate the use of this link and the safeguards currently in place in Q4 2005.

6.2.6 LOW Priority - User IT Security Awareness

Negative impact on system/information confidentiality, integrity and availability.

Technology cannot completely protect networks and systems from security threats. Users are a key component of any security plan and contribute to security through the reporting of security incidents, identification of security weaknesses, and prevention of successful attacks through recognition of dangers of certain types of actions or activities.

The findings were as follows:

- Users who were interviewed during the site visits did not recall the IT Security Awareness material published by IT Security.
- Users who were interviewed during the site visits did recall the IT Security broadcast e-mails warning of malicious activity on the Internet (active viruses and worms such as Slammer, Zotob, etc)

Business Impact

All the security controls in the world will not completely eliminate the vulnerability risk. This is especially true when people are deeply embedded in all processes. When City staff are continuously made aware of the latest security threats, they act as the first line of defense in the City security posture.

Security awareness programs would keep the first line of defense well informed of the latest security threats. They could identify the potential of a malicious e-mail attachment slipping through the security controls. They would leverage their intelligence to recognize harmful attachment signs to prevent opening it, thereby preventing a very embarrassing situation for the City, avoid negative publicity, or avoid legal implications.

Recommendation 17

That Information Technology Services:

- **Create a program with annual user IT Security policy review with mandatory quarterly/semi-annually IT Security awareness briefings;**
- **Continue the Security flash e-mail awareness campaign notifying users of significant e-mail attacks; and**
- **Improve the effectiveness of the IT Security awareness campaign.**

Management Response

Management agrees with these recommendations.

A formal IT Security Awareness program already exists. Awareness articles are issued through City Briefs on a monthly basis, Management Bulletins are also issued as necessary, and IT Security awareness briefings occur to address strategic issues or groups. Awareness activities have been part of the annual planning cycle since 2003. Flash e-mail awareness campaigns will continue.

A third party review to measure and assess the current awareness targets and associated delivery strategy was scheduled to begin October 2005 as part of the Corporate IT Security Awareness Program. This review was deferred to 2006 due to a City-wide budget freeze, and will include specific recommendations and a workplan identifying the priority messaging targets

6.3 Policy Compliance

Policy compliance refers to the observed use of e-mail and Internet browsing by employees compared to the stated policy intent for use of the City's systems. The policy compliance analysis is reported in the following two sections. The first section is the web browsing referring primarily to the HTTP protocol commonly referred to as WWW (World Wide Web). The second section is e-mail compliance reports. Policy compliance does not directly impact on the confidentiality, integrity, or availability of information assets and resources, but rather is a measure of the conformity of the users to the intended and expected use of these services. The Responsible Use policies do state that personal use of these services is accepted provided that such use does not cost the City any additional money (above the cost to provide the service for business use) and that employees use these services for personal use only outside of their business hours.

To perform this analysis, log files and actual content were reviewed to classify each type of visit as either "Business Use", "Personal Use", or "Indeterminate". Each is defined below in section 6.3.1. The classification of the instances of use of the services is based in part on the employee's position compared to the subject of the communication. We performed this classification manually by reviewing both the Websense categories for URLs (universal resource location) or by reviewing actual URLs visited. A URL is the address of a web page on the World Wide Web.

A characteristic of web pages is embedded advertising. Advertisement manifests as sections of a web page that are loaded when the user selects the page. The advertisements often are sourced from different sites than the original web page. Users have no control over advertisement, yet the Websense tool still categorized these as a hit for the user. Most of these hits are classified by Websense as "PG ADS". Therefore to prevent skewing the results, advertisement hits on this particular group have been removed from the analysis and results below.

Finally, there are two distinct groups for which analysis has been performed:

- Random 50 – from across the entire City computer user group, a random selection of 50 user names (employees only, not generic accounts) was selected for analysis. Both e-mail and Internet use was analyzed.
- Top 50 – from across the entire City computer user group, the top 50 user names (employees and generic accounts) were selected for analysis. Top 50 was selected on volume. Only Internet use was analyzed for the top 50, as the e-mail data was not available.

Data for the month of May 2005 was analyzed for the review of Internet usage. Data from a week in September 2005 was used for the e-mail analysis.

For comparison purposes, we also include a summary of Internet usage, as reported by Information Technology Services Branch, for the month of October 2005.

TOP 100 PERMITTED WEBSITES VISITED DURING OCTOBER 2005
Per Information Technology Services Branch

Category (per ITS)	Examples	% of Top 100 Website "hits"	% of Total Internet Traffic (Oct 2005)
Internet Search Engines	www.google.ca kh.google.com cdn.mapquest.com	41.7%	25.9%
Advertising	ad.doubleclick.net adcounter.theglobeandmail.com adme.411.ca	29.3%	18.2%
Sports, Shopping & Entertainment	www.tsn.ca www.mls.ca	5.3%	3.3%
News and Media	OttawaSun.com CBC.ca	4.2%	2.6%
References	weatheroffice.ec.gc.ca www.Isuc.on.ca	2.4%	1.5%
Job Search	Workopolis.com	2.0%	1.3%
Information Technology	download.windowsupdate.com www.microsolft.com	1.6%	1.0%
City of Ottawa Application	Interfleet.ca Library.Ottawa.on.ca	1.2%	0.7%
Other	Includes "uncategorized"	12.2%	7.6%
Totals		**99.9%**	**62.1%**

6.3.1 Internet Policy Compliance Definition

Internet policy compliance refers to communications on the Internet using non-e-mail protocols consisting primarily of a web browser to the World Wide Web.

It is recognized that not all site visits recorded by Websense are intentional visits by a user. In fact, for every intentional visit (a user clicks on a link, or a user enters a URL in the address bar), the potential exists for a number of other unintentional site visits to be recorded by Websense. While this creates challenges for identifying the actual sites visited intentionally by a user, it is possible to use this data to categorize the usage of the Internet by users with some degree of accuracy.

The recording of site visits are also affected by other factors as follows:

- Time since last visit to site and system caching of pages from previous visits.
- Links to other pages such as advertisements, images, frames, and pop ups.
- Pages with dynamic content may also result in additional, unintentional hits based on automatic updates through polling or updates to web pages.
- User visits to sites are summarized within a 15-minute time period.
- Users that leave browsing windows open on sites that periodically reload automatically outside the 15-minute time period, will have multiple hits recorded.

However, even with some weaknesses, Websense is a common tool used in the industry for reporting Internet usage. If Websense is deemed to be not appropriate for reporting purposes, IT may wish to investigate alternate, more effective tools and methods available for this purpose.

Due to the large volume of data to review, the analysis used the site classifications assigned to the site visited by Websense (the content filtering tool in use by the City). These classifications are a number of high-level categories such as Information Technology, Sports, Business and Technology, Travel, Vehicles, Entertainment, etc. Utilizing these categories allowed rapid analysis of the data. For example, categories such as Entertainment and Sports are nearly always personal for most users (the exception was where users assigned to a sports-related job function). In addition, the category “Productivity PG: Advertisements” was eliminated from the analysis since this is almost entirely unintentional site visits.

Furthermore, the site visits were categorized as either “personal” or “business use” on a user’s role or title within the City. For example, Websense classifies www.Microsoft.com as “Information Technology”. For an employee with a position that is related to information technology, visits to sites categorized, as Information Technology will be tallied as a business use. If an employee’s position does not appear to relate to Information Technology (e.g. a shipping clerk) then this visit would be classified as personal. In addition some sites are not categorized by Websense due to the type of content (categorized by Websense as Miscellaneous and therefore not useful to classify). In these cases, we reviewed the site description to determine the classification. Users were also given the benefit of the doubt when there was a question regarding personal use – these items were classified as “indeterminate.”

Site visits were classified as follows:

- Business Use – based on position, the item appears to have been business use (for example, an employee with an IT-related position visiting an Information Technology web site would be classified as business)
- Personal Use – based on position, there is no reason for the user to have visited this category of site
- Indeterminate - based on position, it is not possible to assign the site visits to either business use or personal use

The classification was based on our evaluation of the actual URL that Websense generated for each user.

6.3.2 Random 50 – Internet Compliance

A sample of 50 random user accounts was scrutinized for the month of May 2005. The spread for this group ranged from 44,220 hits (or 2,106 hits per day for the highest user account) to no hits for the lowest user account.

The following results were reached from the analysis of the data on the random 50 users:

- 10 user accounts (20% of total) had no Internet use recorded
- 1 user account (2% of total) had only business use recorded Internet
- 19 user accounts (38% of total) had no business use recorded
- 20 user accounts (40% of total) had a mix of business and personal use
- Average personal use was 53%
- Average business use was 10%
- Average indeterminate use 17%
- Per ITS, users had no data 20%
- The top 10 user accounts accounted for over 80% of Internet activity

6.3.3 Top 50 – Internet Compliance

The Top 50 user accounts were scrutinized for the month of May 2005. The spread for this group differed greatly and ranged from 2,098,002 hits (or 99,905 hits per day for the highest user account) to 29,761 hits (or 1,417 hits per day for the lowest user account).

The following results were reached from the analysis of the data on the Top 50 users:

- 4 user accounts (8% of the total) had all business use recorded, these users were service accounts
- 25 user accounts (50% of the total) had no business use recorded, of these 12 had indeterminate use
- 21 user accounts (42% of the total) had mixed business and personal use. Of these 21 user accounts, 9 had greater than 75% personal use
- Average personal use was 66%
- Average business use was 14%
- Average indeterminate use 20%
- The top 20 users accounted for approximately 80% of Internet activity for this group

One user account in the Top 50 accounted for 44% of the total Internet hits reported for this group, which is dramatically higher that the next user's (at 4.2%). The primary source (98% of this user's activity) of this user's hits was to the Google e-mail site GMAIL.COM. This use violates the City's Policy and is also dangerous in that it is possible to bypass other controls

designed to protect the City network from malicious software. This user is an Ottawa Public Library staff and as such is bound by the Ottawa Public Library's Policy and not the City's Policy.

Internet Usage -The following key points regarding Internet usage can be drawn from the above results of these two sample groups:

The "80/20" rule can generally be applied to the use of the Internet by employees. That is, 80% of the use is generated by 20% of the employees. Both the top 20% of the users of the Internet and the overall City population generated substantially more personal use than business use. In general, large amounts of Internet use is personal. For the random sample, average personal use was 53% and for the Top 50 users it was 66%.

Based on the existing Policy, personal use of the Internet should be performed outside of business hours and the use of the Internet should not incur costs to the City. For our analysis, the time of day that the Internet usage occurred was not available in a suitable format, therefore we were unable to determine if this Internet usage was outside of business hours as permitted by the policy. Monitoring by IT is not done to determine compliance to this restriction.

The Responsible Use of the Internet Policy specifically allows personal use of this corporate resource. While it may be expected that some minimum level of incidental personal usage may occur, we would expect that the level of personal use of the Internet should be similar to the expectations of limited personal use of the telephone. The City's policy on e-mail use only permits incidental personal use of e-mail, similar to the expectation of limited telephone use. Given the high personal use of Internet we found, the City's Responsible Use of the Internet Policy should be revised to limit personal use of the Internet to incidental or occasional only.

6.3.4 Random 50 – E-mail Compliance

The following results were reached from the analysis of the data on the Random 50 e-mail users:

- An average of 16% of e-mails sent or received by the sample was personal – this equates to an average of 21 personal e-mails per person per week
- 10% of the users from the sample had 100% business use of e-mail only
- 78% of the users from the sample had mixed business and personal use of e-mail
- 12% of the users from the sample had mixed business and indeterminate use of e-mail
- 10% of users had more than 50% personal use of e-mail
- 32% of the e-mail sample group (5 day work week) sent or received 5 or more personal e-mails per day
- The top 5 users of personal e-mail sent and received between 15 to 20 personal e-mails per day
- The top 17 users from the sample group generated 80% of all e-mail traffic
- All users had business e-mail traffic

From the above analysis we can conclude that e-mail usage by some employees consists of large amounts of personal e-mails. This usage is in violation of the City's Responsible Computing Policy.

6.3.5 Top 50 – E-mail Compliance

An analysis of the top 50 e-mail users could not be performed, as Information Technology Services was unable to generate an accurate report from this data. The report for the top 50 e-mail users had large blocks of records that were duplicates with only a slight variation in time between entries and could not be used for purposes of our audit. The deficiency in the data could not be explained by Information Technology Services. Since the accuracy of the data was suspect, the report was not used.

We would expect that an organization such as the City of Ottawa would have proven tools to accurately and quickly provide reports such as top e-mail users, random users, sent e-mails, received e-mails, and other e-mail metrics to be used to analyze e-mail usage. Alternative methods to track and monitor high e-mail users should be obtained.

In order for managers to monitor staff to ensure that they are using Internet and e-mail appropriately, managers need to be provided with reports of Internet and e-mail usage. Information Technology Services is responsible for monitoring and controling the use of the Internet and e-mail. This should include a process for reporting high volume or unusual usage patterns to managers so that they may evaluate if appropriate usage has occurred.

6.3.6 Policy Compliance – Internet and e-mail Usage

Recommendation 18

That Information Technology Services:

- **Monitor and control the use of the Internet and e-mail usage by City employees;**
- **Develop appropriate recording tools that provide reliable reporting of e-mail usage;**
- **Implement a process to provide managers with reports of their staff's Internet and e-mail usage so that management can evaluate if appropriate usage of e-mail and Internet is occurring; and**
- **Revise the Responsible Computing Policy to limit use of the Internet to mainly business purposes and limit personal usage to incidental or occasional only.**

Management Response

Management agrees with these recommendations.

IT Services uses Websense to monitor and control the use of the Internet at a macro or system level. Prior to the audit, IT Services launched an extensive project to enhance the rigour of the Websense implementation, scheduled for completion in Q1 2006. An extensive range of additional Websense filtering features is now in place that enhances the monitoring of Internet usage and blocking of websites that are not consistent with the Code of Conduct and Responsible Computing Policy. Monthly reviews of Websense reports by IT Services will continue, and changes to categories, website blocking, and follow-up investigations will continue.

In 2006 IT Services will enhance Internet monitoring using existing Websense reporting tools. A detailed analysis of a minimum of 50 Internet accounts will be conducted on a semi-annual basis for compliance with the Responsible Computing Policy. Instances of non-compliance will be investigated in conjunction with managers and the Labour

Relations unit within Employee Services Branch. It is projected that this level of review and follow-up will generate the equivalent of 1.5 FTEs (2,700 hours) of staff effort to implement.

IT Services/Labour Relations will be contacting the respective managers of the 50 random and 50 top users generated throughout the audit. IT Services in consultation with Labour Relations will provide the Internet log report along with guidelines on how to interpret the data set and how to approach employees with any concerns that might be presented on their Internet usage.

IT Services will continue to produce management reports and metrics using Promodag, and will investigate additional monitoring tools and reporting capabilities that would enable monitoring of individual e-mail accounts. Evidence of non-compliance with the Responsible Computing Policy will be investigated in conjunction with managers and Labour Relations. At this time, the additional effort to review and follow-up is not known pending identification and selection of new tools. A budget pressure would be identified for 2007 to acquire and implement additional monitoring and reporting tools.

The revised Responsible Computing Policy clearly states that the Internet and e-mail are provided for "legitimate business use in the course of assigned duties and only incidentally for personal use", and that disciplinary action, including dismissal, are consequences of non-compliance. The Responsible Computing Policy will be reviewed to ensure that it applies equally to both Internet usage and e-mail usage, and reflects our current practices.

Overall Management Comments

Information Technology Services (ITS) concurs with many of the recommendations proposed by the Auditor General. Where management does not agree with the findings and/or recommendations proposed by the Auditor General, an explanation is provided to substantiate this position. In all cases, this is the result of further research or consultation with vendor suppliers, security experts, and industry best practices.

In cases where management has already commenced an action, a status update has been provided. Where no action has been taken, the proposed timeline and any budgetary implications and expected outcomes have been identified.

The Information Security Strategy (presented to City Council in 2003) described a "risk-management approach" to IT Security to ensure the confidentiality, integrity and availability of City of Ottawa information and IT assets throughout all stages of their lifecycle. At that time, the Strategy was described by the Gartner Group as "far advanced in comparison with other government agencies, and that roles and responsibilities for IM/IT Security are well defined". It is within this context that the following Management Comments address the audit Executive Summary and Findings in more detail.

The City's network is a heterogeneous group of devices that is separated by security controls that enable the City to isolate segments of the network to prevent a security incident from impacting all systems on the network. The effectiveness of this approach is illustrated by examples from the past few years of worm outbreaks that affected businesses throughout the world.

There is also an important distinction to be noted between current practices used by IT Services to monitor and track Internet and e-mail usage, versus the enhanced monitoring proposed by the audit recommendations. IT Services monitors Internet and e-Mail usage and compliance with City policies at a macro level using existing staff resources and best-of-breed software tools. The audit recommendations propose policy changes and enhanced monitoring to an individual level.

At the time of the audit, the Ottawa Public Library is exempt from the City's Responsible Use of the Internet Policy for reasons of intellectual freedom, although OPL staff is network users. Many of the findings and recommendations, particularly related to compliance with City policies, reflect this exemption.

Nevertheless, the increase in frequency and sophistication of both internal and external threats requires continual improvement, attention and investment in order to stay ahead of existing and new threats and vulnerabilities. At this time, the City of Ottawa's IT security posture is further advanced than other Canadian municipalities and many public and private sector organizations.

To implement the recommendations contained within the report requires 5.5 FTEs, including $1.1M of additional base funding, and $1.4M of one-time capital. Further investment in IT security as recommended by the Auditor General would enhance the City's IT security position.

Internet Usage

Internet access is provided to authorized network users for business purposes, however similar to personal use of e-mail and telephone service, there is an expectation that some personal usage will occur. This is consistent with the majority of public and private sector organizations. A recent survey of 25 Canadian municipalities confirmed that more than 80% provided universal access to their staff, and of these organizations, 88% allow personal use.

A review of other surveys and published best practices also provides strong evidence that the majority of organizations (75%) approach the issue of Internet usage by employees through a four-pronged strategy. This has grown from 65% in 2003, and less than 50% in 2001.

Firstly, a policy that defines expectations, what's acceptable/what's not, and what are the consequences for non-compliance. Over 80% of organizations have some form of "acceptable use" policy that defines what the employee can or can't do.

Secondly, education is provided on the policy, the organization's expectations and the consequences of non-compliance. This is essential to avoid vicarious liability – courts look more favourably on organizations that have a policy and regularly educate their employees.

Thirdly, monitoring to ensure compliance with the policy and effectiveness of the education program, and provide feedback for the evolution of the policy. In Canada, while the majority of municipalities monitor usage at a macro level, generally less than 10% of municipalities monitor for personal use vs. business use. This is due to limitations of adequate software tools to make this cost effective. An alternative that is used is a strong emphasis is placed on blocking web sites that are deemed to be inappropriate.

Finally, enforcement is necessary to address non-compliance and deter/discourage inappropriate behaviour.

This is consistent with the approach adopted by the City of Ottawa. The Responsible Computing Policy and accompanying Responsible Use of the Internet Policy provides the City with tools to manage Internet usage, by limiting personal usage to incidental use only, and clearly defining the City's expectations in terms of what the City considers acceptable and appropriate or inappropriate use.

Specific restrictions include sites which are clearly inappropriate for business functions of the City, those that are potentially socially or morally offensive and do not support the operating principles and practices of the City, those that have a strong potential to impact network bandwidth capacity, or those with a strong potential to cause a network security breach. It is very clear that disciplinary actions, including dismissal, are consequences of non-compliance with the Policy.

The network users are regularly reminded of the Policy and their responsibilities every time they log into the City network and/or the Internet. Monthly articles through City Briefs, Management Bulletins and/or flash e-mails are major elements of ongoing user education.

IT Services monitors Internet usage at various levels. Internet traffic is monitored throughout the day to ensure usage falls within generally acceptable parameters (i.e. available network capacity never falls below minimum availability). Unusual traffic patterns are also identified. Websites that are not in compliance with the Policy are blocked. Attempts to access blocked websites are tracked, and on request and investigation by IT Services, may be unblocked if it can be demonstrated access is required for business purposes. The Chief Information Officer meets regularly with IT to review summary Websense reports on Internet usage (permitted sites), attempts to access blocked sites, and requests to un-block sites. Actions taken as a result of this review could include: changes to Websense blocking parameters, additional monitoring or investigation of unusual activity that would indicate non-compliance with City policies.

Presently, it is not the mandate of IT Services to monitor individual employee usage of the Internet. Monitoring of staff activity is the responsibility of managers and supervisors. While current Websense reporting tools accurately track Internet "hits", it is a manual labour intensive process to review detail reports to remove automatically generated "hits" (advertising, web counters, etc.) from legitimate websites. It is also difficult to determine with reasonable certainty whether a legitimate website is being used for business or personal use. This is particularly problematic given the diverse lines of business and job functions of City staff. What would be considered "personal" for most staff could be "business" for others. Examples might include ebay.com or MLS.com – both are used by City staff involved in procurement activity and property valuations.

Where there is evidence of non-compliance with the policy, an investigation is launched to determine whether there has in fact been a breach of policy. In some cases, the investigation is informal and related to unusual levels of Internet activity that can be readily explained or don't indicate abuse. In other cases, IT Security may be approached by a Manager/Labour Relations to investigate potential abuse by an employee. Through 2002-2005, IT Services investigated 30 instances of inappropriate use of the City's Internet/e-mail services on behalf of managers.

Information Technology reviewed the Auditor's findings that the average personal use of the Internet for a random sample of 50 user accounts is 53%. Based on generally accepted sampling techniques, management

believes that a larger sample size (e.g., 365-370) would be appropriate for a population of 9,000 users to achieve a 95% confidence level, particularly if the results are to be used to substantiate significant policy changes.

Management also notes that a significant percentage (40%) of total Internet usage is in fact "noise" - sites that are not generated by a user's input (mouse click), but may be generated unintentionally. This included web counters, advertising, pop-ups, and image servers.

It is not possible to determine from the top 100 sites whether they are visited for personal or business purposes. However, it is evident that only a few categories (e.g., Sports, Shopping and Entertainment) are most likely for personal use. Other categories such as News and Media could be a mix of personal/business. Other categories are clearly business-related (e.g., Job Search: workopolis.com).

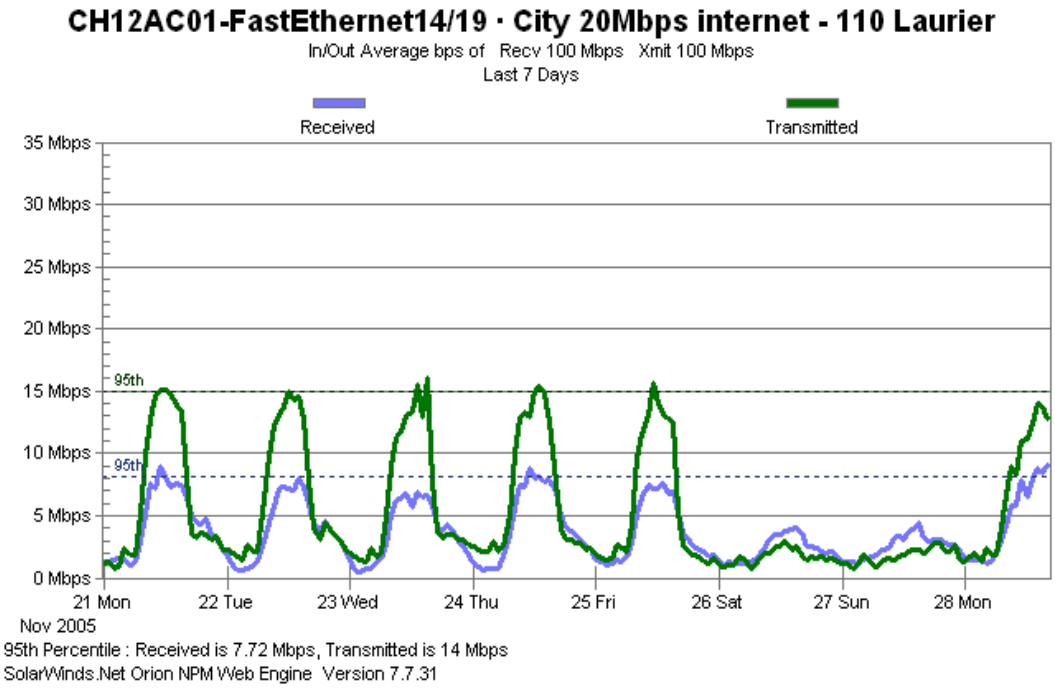
Management is also concerned that certain sites (e.g., Microsoft.com) would be considered business use for IT staff but personal for other staff. There are at least four instances where visits to Microsoft.com could be considered legitimate business.

1. Selecting the Help command in Microsoft Word, for example, enables the user to connect to Microsoft.com for technical resources or further information on Word.
2. Laptop users are periodically prompted to download and install security updates that require connection to Microsoft.com.
3. Windows Media Player (required for webcasting/video-on-demand) often generates an Internet visit to Microsoft.com that notifies users that updates are available.
4. Microsoft.com is a major source of images and clip-art used by City staff for presentations, preparation of materials for the public.

Nevertheless IT Services reviewed detailed usage reports for a subset of 16 users from the 50 random users. The 16 users were determined by grouping the random 50 by Department/Branch, and by selecting the largest three groups/Branches. Management assessed their Internet usage following a methodology similar to that used by the Auditor. Management determined that based on the 16 users, the percentage of personal use was 56%, slightly higher than the audit findings.

On more detailed examination, it was found that one user had unusually high usage relative to the others, of which 94% was categorized as personal usage. This was determined to be a significant amount of streaming video. By eliminating this user from the sample, the percentage of average personal use dropped to 11%.

Analysis of daily Internet traffic reports shows that Internet use generally peaks during the period of 11am – 2pm, suggesting that personal usage is likely occurring during lunch breaks. This is substantiated to some extent by the above analysis of 16 users, which showed personal use (e.g. on-line banking) occurring outside normal working hours.



E-Mail Usage–General Management Comments

Information Technology Services uses a product called Promodag to generate various e-mail related metrics. The Promodag system is designed to generate reports that measure the usage of the electronic messaging system and help analyze traffic patterns. Promodag is not able to produce the type of reports requested by the Auditor to monitor staff email usage for content and compliance with City policies.

Promodag reports generated monthly include:

- Usage of Distribution Lists
- Breakdown of mailboxes by size
- Daily average of messages transmitted
- Message delivery times
- Size of message breakdowns
- Internal and external traffic volumes, sent and received, by numbers of messages and size

The system also generates mailbox traffic reports using key parameters. For example:

- All mailboxes with 500+ external messages sent in a given month.
- All mailboxes with 500+ external messages received in a given month.

Promodag is limited in its ability to provide detailed audit reports for individual mailboxes showing details such as subject line, time received / sent, etc. on a per e-mail basis. Custom reports can be produced but require the expertise of a SQL database specialist.

Using automated tools to monitor staff e-mails is not a common organizational practice. However, with the growing concern regarding leakage of confidential information and compliance with regulatory policies such

as Sarbanes-Oxley (particularly in the United States), technology is evolving to provide organizations with better tools to monitor e-mail content. However, the focus is on preventing accidental or intentional leakage of confidential information to unauthorized recipients.

Policy Compliance - General Management Comments

IT Services has not reviewed the specific instances of non-compliance noted during the course of the audit, but concurs with the audit findings in general.

IT Services is aware of specific instances where some degree of non-compliance has been identified, and as noted above, have been involved with investigations of non-compliance with Managers and Employee Services (Labour Relations).

It is important to understand Ottawa Public Library staff was exempt from the Responsible Use of the Internet policy at the time of the audit. These users would in fact be compliant with OPL policy, but non-compliant with the City Policy. In particular, ITS monitoring of the Internet identified non-compliance with the City Policy that upon further investigation was a result of Library users who are not subject to the same degree of filtering as other City staff (e.g., non-City e-mail accounts and systems, web chat).

IT Services monitors and tracks Internet usage at a macro level, but has not monitored individual employees unless requested as part of an investigation into alleged abuse of the Policy. Monitoring individual employee usage is a labour-intensive activity. The City relies primarily on Websense to ensure users remain in compliance with the Policies by blocking web sites that would result in non-compliance. As noted by the audit findings, Websense has generally been effective in blocking websites that are not permitted by Policy or have a negative impact on productivity. As previously noted, in 2005, prior to the audit, IT Services launched an extensive project to enhance the rigour of the Websense implementation, and an extensive range of additional Websense filtering features is now in place.

In some instances, lack of compliance would be evident from users visiting websites that are incorrectly categorized by Websense and therefore are not blocked. As these are identified, IT Services re-categorizes these sites to prevent future access (e.g., Personal and Dating).

Conversely, web sites that are not permitted (and therefore blocked) may be un-blocked for certain staff on request, following investigation by IT Services to confirm that they are required for business purposes (e.g., eBay.com, MLS.com).

Shared accounts and sharing of account passwords are prohibited by Policy, but on an exception basis, shared accounts are permitted to enable staff to administratively support City applications, systems and business requirements. However, IT Security reviews all requirements for shared accounts and maintains records on these accounts.

7.0 Conclusion

This audit reviewed the adequacy, effectiveness and reliability of security measures and controls in place over the usage of the Internet and e-mail and assessed whether Internet and e-mail usage is compliant with City policies. While security controls currently implemented were found to be generally effective and reliable, there were gaps in the adequacy of the controls. The audit also reviewed the compliance of usage of the Internet and e-mail to the current policy statements and found that there is considerable personal use of these tools. The Responsible Use of the Internet Policy and the Responsible Computing Policy should be revised to limit the use of the Internet to mainly business purposes and limit personal usage to incidental or occasional only. A program to monitor and control Internet and e-mail usage should also be established.