Martin Matson
Comptroller

John M. Egan, CPA
Deputy Comptroller

Glenn Steinbrecher, CPA
Special Deputy Comptroller

Toni Biscobing
Special Deputy Comptroller

Office of the Comptroller

July 31, 2013

To the Honorable
The Common Council
City of Milwaukee

Dear Council Members:

Anti-virus controls, through the proper use and configuration of various third party applications, are an important and necessary part of ensuring that the City of Milwaukee's (City) computer systems are available, and that City services connected to computing resources are not impaired. A department's network must therefore maintain high standards for ensuring the security, integrity and functionality of its hosted computer environment, and that it is safe from harmful viruses.

In the current computing environment, an unprotected computer or network is not only vulnerable, but is likely already infected. Ten years ago computer viruses[i] and malware[ii] were written by technology savvy people to show off their skills, and were more a nuisance than harmful to computers. Since then viruses have been transformed into a multimillion dollar industry fueled by organized crime and hostile nations. The current threat targets financial and personal information and can often remain on a system for years without being discovered. Local municipalities around the country have recently been targeted by foreign nations, as was the case in Massachusetts and Florida during the previous presidential convention. The anonymous hacker group loosely affiliated with the Occupy Wall Street movement has also been known for cyber-attacks[iii] on local municipalities.

The City of Milwaukee takes these threats seriously. To assess the strength of the City's anti-virus protection, the Audit Division conducted an anti-virus audit in February, 2013.

The audit examined eleven anti-virus controls in five different City departments: Information Technology Management Division, Fire Department, Police Department, Library, and the Department of City Development. An anti-virus survey was also sent to other City departments to ascertain that they have implemented an anti-virus software solution. Audit meetings and system testing were completed by in-person testing and screen print captures at the five departments.

Tested controls included:

- Verification of the most current anti-virus programs being applied to the network and its computers.
- Verification that virus definitions[iv] are applied to computers automatically on a regular basis.
- Verification that anti-virus software is configured to scan all files including internet downloads, compressed ZIP files[v] and emails for virus threats.
- Verification that automatic weekly full system scans[vi] for viruses are taking place.
- Verification that heuristic[vii] virus checking is taking place to prevent zero-day[viii] attacks.
- Verification that anti-virus software is configured to automatically repair infected files.
- Verification that anti-virus software is configured to automatically enable upon computer start up.

The audit also included the introduction of two mock viruses to test the anti-virus software's efficacy in identifying and eliminating a virus threat.

The City currently uses many different anti-virus solutions that are widely available on the market. These programs include: McAfee, AVG, Sophos, Trend Micro, Symantec and others. The audit's objective was to verify that these software solutions were configured to information technology security best practices which include: automatic daily virus definition updates, configuration to scan all file types, at least weekly full system scans, the implementation of heuristic threat checking to prevent zero-day attacks, and that the anti-virus programs start up automatically when a computer is booted up[ix].

The anti-virus survey results showed that all surveyed departments and divisions have implemented an anti-virus software solution. City departments have multiple contracts with software vendors to use their anti-virus software, often on a per user cost basis. If the City decided to use one anti-virus software and purchased the licenses together, it would gain greater bargaining power and lower the overall cost of virus protection. There are challenges in this kind of decision implementation as the current anti-virus contracts all terminate at different times, but most will conclude within the next two years.

The Audit Division's general opinion is that the sampled departments' anti-virus protection is in good operational standing and that scheduled, automated, and configuration controls are operating effectively with few exceptions.

Three exceptions were identified as a result of this audit and recommendations for improvement have been communicated to the appropriate City personnel.

The Fire Department currently uses AVG anti-virus software, which is a reputable product but is not configured for strong security when it applies to scanning all downloaded and present files, including compressed ZIP files. Due to this misconfiguration of security settings the two mock viruses that were introduced into the Fire Department's network were not detected and neutralized.

1. **The Fire Department's AVG anti-virus software is not currently configured to scan all internet downloads.**

   Recommendation: The "scan all files" radio button in the software configuration settings should be selected to allow the software to scan all incoming files.

2. **The Fire Department's AVG anti-virus software is not currently configured to scan all files during scheduled system scans.**

   Recommendation: The "All file types" radio button in the software's computer scan settings should be selected to allow the software to scan all present files on the network.

3. **City departments are currently using a variety of anti-virus software solutions. This makes it difficult to enforce a single standard for security configurations and could be resulting in higher licensing costs.**

   Recommendation: The Information Technology Management Division (ITMD), with the help of the City Information Management Committee, should conduct a formal evaluation of whether significant cost savings and operational efficiencies could be achieved by selecting a single anti-virus solution for the entire City. Consideration should be given to centralizing the purchasing and distribution of the licenses within ITMD.

Detailed findings and recommendations were sent to the anti-virus Information Security managers and written responses on the status of the each recommendation have been requested and received. Management is in agreement with all findings.

Appreciation is expressed for the cooperation extended to the auditors by the staff of the departments that were involved in this audit.

Sincerely,

Aycha

Aycha Sirvanci, CPA
Audit Manager

AS:il

cc:
Nancy Olson, Chief Information Officer
Fire Chief Mark Rohlfing
Police Chief Edward Flynn
Paula Kiely, Library Director
Rocky Marcoux, Commissioner, Department of City Development

Attachment: [Glossary of Terms]

Glossary of Terms

Webopedia: Online Computer Dictionary for Computer and Internet Terms and Definitions. N.p., n.d. Web. 5 July 2013.

[i] A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.

[ii] Short for ***mal**icious soft**ware***, malware refers to software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.

[iii] An attack that is designed to bring a network or service down by flooding it with large amounts of traffic. Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests.

[iv] Antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered.

[v] A type of file that contains other files that have been compressed (typically through a ZIP program) for more efficient transfer of the data.

[vi] A function of an antivirus program that searches a system for virus signatures that have attached to executable programs and applications such as e-mail clients. A virus scanner can either search all executables when a system is booted or scan a file only when a change is made to the file as viruses will change the data in a file.

[vii] Heuristics is a technique designed for solving a problem more quickly when classic methods are too slow, or for finding an approximate solution when classic methods fail to find any exact solution. This is achieved by trading optimality, completeness, accuracy, or precision for speed.

[viii] An exploit that takes advantage of a security vulnerability on the same day that the vulnerability becomes publicly or generally known. Zero-Day exploits are usually posted by well-known hacker groups. Software companies may issue a security bulletin or advisory when the exploit becomes known, but companies may not be able to offer a patch to fix the vulnerability for some time after.

[ix] Short for *bootstrap,* the starting-up of a computer, which involves loading the operating system and other basic software.