REPORT OF EXAMINATION | 2018M-146

City of Tonawanda

Information Technology

NOVEMBER 2018

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

City of Tonawanda

Audit Objective

Determine whether the Common Council (Council) ensured information technology (IT) assets were properly safeguarded.

Key Findings

- The Council has not adopted an acceptable use policy or implemented procedures to properly monitor computer use.
- City officials did not maintain an inventory of IT assets.
- City employees were not provided with IT security awareness training.

In addition, sensitive IT control weaknesses were communicated confidentially to City officials.

Key Recommendations

- Establish an acceptable use policy, distribute it to all City personnel and monitor IT usage.
- Maintain an inventory of IT assets.
- Ensure that all necessary City personnel receive IT security awareness training and that training is provided whenever the IT policies are updated.

City officials agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

Background

The City of Tonawanda (City) is located in Erie County. The Common Council (Council), composed of five elected members, is responsible for overseeing the City's operations and finances including establishing policies and procedures to safeguard IT assets and provide a secure IT environment. The Mayor is the City's chief executive officer and is responsible for supervising City officers and employees.

The Council appointed one employee to act as Network Administrator.

Quick Facts	
Employees	162
Residents	15,130
2018 General Fund Appropriations	$22.3 million
Computers	75
Servers	6 physical 4 virtual

Audit Period

January 1, 2017 – April 26, 2018

Information Technology

The City relies on its IT system for Internet access, email, and maintaining and accessing personal, private or sensitive information (PPSI)[1] including financial and personnel records. Therefore, the IT systems and data are valuable City resources. If IT systems are compromised, the results could range from inconvenient to severe and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of an IT system, a lack of effective controls significantly increases the risk that data, hardware and software may be lost or damaged by inappropriate access and use.

How Should IT Assets Be Safeguarded?

The Council should establish computer policies that take into account people, processes and technology, communicate the policies throughout the City's departments and ensure City officials develop procedures to monitor compliance.

An acceptable use policy (AUP) should be in place to describe appropriate and inappropriate use of IT resources and explain management's expectations about personal use of IT equipment and user privacy. Computer use for Internet browsing and email increases the likelihood of exposure to malicious software that may compromise data confidentiality. City officials can limit such vulnerabilities by restricting personal use of IT assets. A clearly stated and communicated AUP also holds users accountable for improperly using City resources.

City officials should maintain detailed, up-to-date inventory records for all computer hardware, software and data. The information maintained for each piece of equipment should include a description of the item including the make, model and serial number; the name of the employee to whom the equipment is assigned, if applicable; the physical location of the asset; and relevant purchase or lease information including the acquisition date. Software inventory records should include a description of the item including the version and serial number, a description of the computers on which the software is installed and any pertinent licensing information.

New York State Technology Law[2] requires the City to have a breach notification policy or local law that requires certain individuals to be notified when there is a system security breach involving private information.

1 PPSI is any information which – if subjected to unauthorized access, disclosure, modification, destruction or disruption of access or use – could severely affect critical functions, employees, customers, third parties or residents of New York State in general.

2 New York State Technology Law Section 208

The Council should require, and provide employees and officials the opportunity to attend, periodic IT security training that explains the proper rules of behavior for using IT systems and data. Security awareness training communicates IT security expectations to employees, helps them recognize security concerns and react appropriately, and helps them understand their individual responsibilities.

Also, a disaster recovery plan (DRP) should be adopted to anticipate and plan for an IT disruption involving the corruption or loss of data. The plan should be tested to ensure that employees understand their roles and responsibilities in a disaster situation. A DRP, sometimes referred to as a business continuity plan or business process contingency plan, describes the plans, policies, procedures and technical measures for the recovery of IT operations after a destructive event, whether a natural disaster (such as a flood), human error, hardware failure or malfunctioning software caused by malware or a computer virus. Periodic backup of critical systems and data is essential to recovery of operations. Backup media should be stored in a secure offsite location that is not subject to the same risks as the onsite assets.

Officials Have Not Properly Monitored the Use of City Computers

The Council has not adopted an AUP. We reviewed 11 computers for non-business use and found evidence of personal use on seven computers. Such use included personal email, personal banking, social networking, online shopping, browsing travel and entertainment websites and other questionable Internet use. When employees access websites for non-business or inappropriate purposes through the network, productivity is reduced and there is an increased risk that City assets and users' information could be compromised through malicious software infections.

We also reviewed these 11 computers and five servers for malicious software and potentially unwanted programs. We found three computers had potentially unwanted programs but none of the tested computers or servers had possible malicious software programs. Potentially unwanted programs can sometimes lead to similar issues, and can unnecessarily consume system resources and decrease productivity when used by employees.

City Officials Did Not Maintain an Inventory of IT Assets

City officials did not maintain an inventory of IT assets. Prior to our audit, the Network Administrator documented the location of IT assets on the purchase order/invoice at the time of purchase but did not maintain inventory records for all computer hardware, software and data. City officials cannot properly protect computer resources, including data, if they do not know what resources they have and where those resources reside. Without detailed, up-to-date hardware, software and data inventory records,there is an increased risk of loss, theft or

misuse of IT assets. Without proper identification of all devices on a network, unauthorized devices and software can be easily introduced, putting organizational data at risk.

During our fieldwork, City officials[3] created an inventory listing of the City's hardware IT assets. This inventory included the location/user, the computer make, model, and serial number, the monitor, printer and any other devices assigned to the user. City officials should continue to maintain this inventory and expand it to include software and the location of essential computerized data.

The Board Has Not Adopted a Breach Notification Policy

The Council and City officials have not developed and adopted a breach notification policy or local law because they were unaware of this requirement. As a result, if private information is compromised, officials may not understand or fulfill the City's legal obligation to notify affected individuals.

Employees Were Not Provided With IT Security Awareness Training

City employees were not provided with IT security awareness training to ensure they understood how to help protect IT assets and computerized data. As a result, there is an increased risk that users will not understand their responsibilities. This can place the data and computer resources with which they have been entrusted at greater risk for unauthorized access, misuse or abuse.

The Board Has Not Adopted a Written Disaster Recovery Plan

The Council and City officials have not developed and adopted a written DRP. Although the servers and financial data are backed up on a regular basis, backups are stored locally rather than offsite. Personnel also have no guidelines to minimize the loss of equipment or implement data recovery in the event of a disaster. Further, City officials do not have a regular method in place for testing backups. City officials stated that backups have been tested periodically when users request the restoration of certain files or information.

Without a formal written plan, all responsible parties may not be aware of steps they should take, or how to continue doing their jobs, to resume business after a disruptive event.

3 The Network Administrator with assistance from departmental employees

What Do We Recommend?

The Council and City officials should:

1. Develop and adopt an acceptable use policy and design and implement procedures to monitor the use of IT resources, including personal use.

2. Continue to maintain an inventory of IT assets and expand it to included software, servers and data.

3. Develop and adopt a written breach notification policy requiring that notification be given to certain individuals if there is a breach of the security of the system involving private information.

4. Ensure all necessary personnel receive IT security awareness training, and update the training whenever the IT policies are updated.

5. Develop and adopt a written disaster recovery plan and written backup procedures that address periodically testing backups and storing the backup media at an offsite location.

Appendix A: Response From City Officials

CITY OF TONAWANDA
LITTLE CITY - BIG COMMUNITY

CITY OF TONAWANDA, NEW YORK
OFFICE OF THE MAYOR
200 Niagara Street Tonawanda, New York 14150 – 1099
Phone: (716) 695 – 8645 Fax: (716) 695 – 8314
E-mail: mayor@tonawandacity.com

RICK DAVIS
Mayor

CHARLES GILBERT
Administrative Assistant

CAITLIN RECH
Executive Secretary

November 13, 2018

To Whom It May Concern,

This letter is in response to the audit performed by your officer, [redacted] on October the 11th of 2018. Below is our plan based on the recommendations in the letter:

1. *Develop and adopt an acceptable use policy and design and implement procedures to monitor the use of the IT resources, including personal use.*

The City is in the process of speaking with surrounding municipalities and obtaining a copy of their policies to use as a template. When this policy is created, it will be put in front of Council for approval and adoption.

2. *Continue to maintain an inventory of IT assets and expand it to include software, servers and data.*

Inventory was performed during the state audit and it will be kept up to date with continued software licensing updates as well.

3. *Develop and adopt a written breach notification policy requiring that notification be given to certain individuals if there is a breach of the security of the system involving private information.*

The City is in the process of speaking with surrounding municipalities and obtaining a copy of their policies to use as a template. When this policy is created, it will be put in front of Council for approval and adoption.

4. *Ensure all necessary personnel receive IT security awareness training, and update the training whenever the IT policies are updated.*

The City is in the process of developing a policy to train its employees on IT securities. This training will be conducted on a yearly basis and will be updated whenever policies are updated.

5. *Develop and adopt a written disaster recovery plan and written backup procedures that address periodically testing backups and storing the backup media at an offsite location.*

The City currently does backups on all of its data and is looking to move this backup system to an offsite location within the year. Once this system is in place, a written disaster plan will be implemented and will included periodic testing.

Kindly,

_____

Mayor, City of Tonawanda

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We interviewed City officials and employees to obtain an understanding of IT operations.
- We inquired about IT related policies and procedures and reviewed written policies and procedures to obtain an understanding of controls over IT assets and operations.
- We judgmentally selected a sample of 11 computers, from approximately 75 computers in total, and five servers (three physical servers, one of which included three virtual servers) from the City's six physical and four virtual servers. Our purpose was to examine and analyze the web browsing histories (computers only) to determine whether employees were using their computers for personal use or if any unwanted or malicious software was present. Our sample was based on risk and included computers/servers used by employees with access to financial records, and one computer from each of the other departments: Mayor, Public Works, Recreation, Fire, and Building.

Our audit also examined the adequacy of certain information technology controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to City officials.

We conducted this performance audit in accordance with GAGAS (generally accepted government auditing standards). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. We encourage the Council to make the CAP available for public review in the City Clerk's office.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/lgli/pdf/cybersecurityguide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/localgov/researchpubs/index.htm

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/localgov/academy/index.htm

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/localgov/index.htm

Local Government and School Accountability Help Line: (866) 321-8503

BUFFALO REGIONAL OFFICE – Jeffrey D. Mazula, Chief Examiner

295 Main Street, Suite 1032 • Buffalo, New York 14203-2510

Tel (716) 847-3647 • Fax (716) 847-3643 • Email: Muni-Buffalo@osc.ny.gov

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming counties

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller