REPORT OF EXAMINATION | 2018M-114

Town of Lancaster

Information Technology

AUGUST 2018

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

Contents

Report Highlights

Town of Lancaster

Audit Objective

Determine whether the Board ensured Information Technology (IT) assets were properly safeguarded and secured.

Key Findings

- Town officials have not designed or implemented procedures to monitor compliance with the acceptable use policy or determine the amount of employees' personal use.
- Town officials did not maintain an inventory of IT assets.
- Employees were not provided with IT security awareness training.

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

Key Recommendations

- Ensure the acceptable use policy is distributed to all personnel and monitor IT use.
- Develop and maintain an inventory of IT assets.
- Ensure all necessary personnel receive IT security awareness training and that training is provided whenever the IT policies are updated.

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

Background

The Town of Lancaster (Town) is located in Erie County. The Town is governed by an elected Town Board (Board) composed of four Council members and a Supervisor. The Board is the responsible for overall operations and finances including establishing policies and procedures to safeguard IT assets and provide a secure IT environment.

Town officials contract with a consultant for IT services including support, network management and a variety of other services. The contract covers the departments located in the town hall, the Police Department and Justice Court. The remaining departments; such as Highway, Recreation, Youth Bureau and Senior Center obtain IT services on an as needed basis.

Quick Facts	
Employees	170
Residents	41,604
2017 General Fund Appropriations	$10.4 million
Payments to IT Consultant (2016-17)	$164,000
Computers	128
Servers	5 physical 7 virtual

Audit Period

January 1, 2016 – December 15, 2017

Information Technology

Town officials rely on the IT system for Internet access, email and maintenance and access to personal, private or sensitive information (PPSI)[1] including financial and personnel records. Therefore, the IT systems and data are valuable resources. If IT systems are compromised, the results could range from an inconvenience to a catastrophe 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 systems may be lost or damaged by inappropriate access and use.

How Should IT Assets Be Safeguarded?

A board should establish computer policies that take into account people, processes and technology; communicate these policies throughout the departments; and ensure town officials develop procedures to monitor compliance with the policies.

An acceptable use policy should be in place which describes appropriate and inappropriate use of IT resources and explains expectations concerning 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. Town officials can limit such vulnerabilities by restricting personal use of IT assets. It can also be used to hold users accountable for improperly using resources.

The Board-adopted acceptable use policy states that minimal personal use of computers, networks, Internet services and email services is permitted as long as such use does not interfere with the employee's job duties and performance, system operations or other system users. It also states that anything beyond 10 minutes per day is considered excessive. This policy further states that employees shall not install, or attempt to install, whether for personal or Town use, on any computer or system, any software or shareware downloaded from the Internet, without first consulting with the outside computer administrator and receiving approval from their respective department head.

Town officials should maintain detailed, up-to-date inventory records for all computer hardware, software and data. The information maintained for each piece of computer equipment should include a description of the item (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

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.

should include a description of the item including the version and serial number, a description of the computer(s) on which the software is installed and any pertinent licensing information.

New York State Technology Law[2] requires a town 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.

A board 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 and communicate the policies and procedures that need to be followed. Security awareness training communicates IT security expectations to employees and helps individuals recognize security concerns and react appropriately. It also helps to ensure that employees understand their individual roles and responsibilities.

A disaster recovery plan should be adopted to anticipate and plan for an IT disruption involving the corruption or loss of data and the plan should be tested to ensure that employees understand their roles and responsibilities in a disaster situation. Such a plan, sometimes referred to as a business continuity plan or business process contingency plan, describes the plans, policies, procedures and technical measures for recovering IT operations after a destructive event – whether a natural disaster (such as a flood) or human error, hardware failure or malfunctioning software caused by malware or a computer virus.

Town Officials Did Not Properly Monitor Computer Use

The Board adopted an acceptable use policy in July 2016. However, officials have not designed or implemented procedures to monitor compliance with the policy or determine the amount of employees' personal use.

We reviewed 18 computers for non-business use and found evidence of personal use on 15 computers. Such use included personal email, personal banking, social networking, online shopping, visiting travel websites, browsing entertainment sites and other questionable Internet use. When employees access websites for nonbusiness or inappropriate purposes through the network, productivity is reduced and there is an increased risk that IT assets and users' information could be compromised through malicious software infections.

We also reviewed these computers and five servers for malicious software and potentially unwanted programs. One computer had a possible malicious software program, and all of the servers and 17 computers contained potentially unwanted programs.

2 New York State Technology Law, Section 208

Malicious software can result in issues that range from a nuisance to theft of personal information or a completely inoperable computer. Potentially unwanted programs can sometimes lead to similar issues, and can unnecessarily consume system resources and decrease productivity when used by employees.

Town Officials Did Not Maintain an Inventory of IT Assets

Town officials did not maintain an inventory of IT assets. The IT consultant has a list of computers and servers, which are maintained under the managed services agreement with the Town. However, this list does not include the computers in departments not covered by the service agreement including the Highway, Recreation, Youth Bureau and Senior Center.

Town officials are unable to properly protect computer resources, including data, if they do not know which resources they have and where those resources reside. By not maintaining detailed, up-to-date hardware, software and information 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 the Town's data at risk.

The Board Has Not Implemented a Breach Notification Policy

The Board and Town officials have not developed, adopted and implemented 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 Town's legal obligation to notify affected individuals.

Employees Were Not Provided With IT Security Awareness Training

Employees were not provided with IT security awareness training to ensure they understand how they could help protect IT assets and computerized data. During our audit fieldwork, the email passwords of at least four employees were compromised in a phishing attack.[3] Had these employees been provided with adequate security awareness training, this attack may not have been successful.

By not providing IT security training there is an increased risk that users will not understand their responsibilities, putting the data and computer resources with which they have been entrusted at greater risk for unauthorized access, misuse or abuse.

3 Phishing attacks use fake email messages typically providing links to counterfeit websites and requesting information such as names, passwords and account information.

The Board Has Not Implemented a Written Disaster Recovery Plan

The Board and Town officials have not developed, adopted and implemented a written disaster recovery plan. Although the servers and financial data are backed up on a regular basis, and backups are stored locally as well as offsite, personnel have no guidelines to minimize the loss of equipment or how to implement data recovery in the event of a disaster. While the servers under contract with the IT consultant are backed up on a regular basis and tested daily, the rest of the departments do not have a regular method in place to perform and test backups.

However, without a formal written plan, all responsible parties may not be aware of where they should go, or how they will continue to do their jobs, to resume business after a disruptive event.

What Do We Recommend?

The Board and Town officials should:

1. Design and implement procedures to monitor the use of IT resources including personal use.

2. Periodically review all computers and remove any malicious software and other unwanted programs.

3. Develop and maintain an inventory of IT assets.

4. Develop, adopt and implement a written breach notification policy requiring that notification be given to certain individuals if there is a system security breach as it relates to PPSI.

5. Ensure all necessary personnel receive IT security awareness training and that training is provided whenever the IT policies are updated.

6. Develop, adopt and implement a written disaster recovery plan and written backup procedures.

Appendix A: Response From Town Officials

Town of Lancaster

OFFICE OF THE SUPERVISOR

21 Central Avenue
Lancaster, New York 14086
(716) 683-1610
Fax: (716) 683-0512

JOHANNA M. COLEMAN
Supervisor

August 13, 2018

Jeffrey D. Mazula
Chief Examiner of Local Government and
School Accountability
Office of the State Comptroller
Buffalo Regional Office
295 Main St. Suite 1032
Buffalo NY 14203-2510

Dear Mr. Mazula:

The following is the Town of Lancaster's response to each of the recommendations in the Draft Information Technology Report of Examination (2018M-114) (the Report) received from you on July 13, 2018.

Recommendation: Design and implement procedures to monitor the use of IT resources including personal use.

Response: The Town agrees that IT use should be monitored. The Town's IT consultant currently has the ability to monitor employee personal computer use upon request of the Town.

Recommendation: Periodically review all computers and remove any malicious software and other unwanted programs.

Response: The town agrees with this recommendation. All computers are monitored by the Town's IT consultant and all have software installed designed to alert the users not to install malicious software. In some cases, older versions of certain programs which could be considered to be potentially unwanted are required to be and intentionally are installed in order to support certain older but fully functional programs currently used by town personnel.

Recommendation: Develop and maintain an inventory of IT assets.

Response: The Town agrees with this recommendation and has addressed it. As discussed in the report, the Town's IT consultant previously had only a list of computers and servers which were monitored under the managed services agreement that was maintained with only certain Town departments. However, the Town Board recently approved a new managed services agreement that covers all Town

departments so, accordingly, the Town's IT consultant has created and will maintain an inventory of all IT assets, as recommended.

Recommendation: Develop, adopt and implement a written breach notification policy requiring that notification be given to certain individuals if there's a system security breach as it relates to PPSI.

Response: The Town agrees with this recommendation. As discussed in the Report, town officials were not aware that the New York State Technology Law had such a requirement but will be working with the Town Attorney to come into compliance with the law.

Recommendation: Ensure all necessary personnel receive IT security awareness training and that training is provided whenever the IT policies are updated.

Response: The Town agrees with this recommendation and is evaluating ways to provide such training to Town employees.

Recommendation: Develop, adopt and implement a written disaster recovery plan and written backup procedures.

Response: The Town agrees with this recommendation. The Town has a disaster recovery plan and backup procedures but to date, has not reduced it to writing.

If you have any questions, please feel free to contact me.

Very truly yours,

Johanna M. Coleman
Supervisor

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 Town officials, employees and the IT consultant 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 18 computers (from 128 computers in total) to examine and analyzed the web browsing histories to determine whether employees were complying with the acceptable use policy. Our sample was based on risk and included computers used by employees with access to financial records and computers not being serviced by the IT consultant.
- We performed authenticated scans against a judgmental sample of 18 computers (from 128 computers in total) and five servers (two physical servers, one of which included four virtual servers from the Town's five physical and seven virtual servers) to identify the software installed and settings configured. We analyzed the scan results for security weaknesses. Our sample was based on risk and included computers/servers used by employees with access to financial records and computers/servers not being serviced by the IT consultant.

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 Town 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 relevant population size 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 Board to make the CAP available for public review in the Town 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