DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2018M-156

Town of East Otto

Information Technology

OCTOBER 2018

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

Contents

Report Highlights

Town of East Otto

Audit Objective

Determine whether the Board ensures that information technology (IT) assets are properly safeguarded and accessed for appropriate Town purposes.

Key Findings

The Board has not:

- Adopted an acceptable use policy; we found evidence of personal use on four of the six computers examined.
- Adopted a disaster recovery plan or formal backup procedures.

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

Key Recommendations

- Adopt an acceptable use policy describing inappropriate and acceptable use.
- Develop, adopt and implement a disaster recovery plan and formalize backup procedures.

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

Background

The Town of East Otto (Town) is located in Cattaraugus County. The Town is governed by an elected Town Board (Board), which is composed of a Supervisor and four Council members. The Board is responsible for the general oversight of operations and finances, including security over the Town's IT system.

Quick Facts

Residents	1,100
2018 Appropriations	$1.2 million
Employees	13
Computers	6

Audit Period

January 1, 2017 – May 15, 2018

Information Technology

Town officials rely on IT resources for Internet access, email, and maintenance and access to personal private or sensitive information (PPSI)[1] including financial, personnel and Justice Court records. Therefore, the IT systems[2] and data are valuable resources. If IT systems are compromised, the results could range from 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 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 town's departments; and ensure town officials develop procedures to monitor compliance with 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.

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.

New York State Technology Law[3] 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.

[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] Town officials use individual MiFi devices or their personal Internet connection; therefore, the Town does not have a network.

[3] New York State Technology Law, Section 208

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.

The Board Did Not Adopt an Acceptable Use Policy

The Board and Town officials have not developed, adopted and implemented an acceptable use policy addressing the appropriate and inappropriate uses of IT resources, and expectations concerning personal use and user privacy. We reviewed all six computers for non-business use and found evidence of personal use on four computers. Such use included personal email, social networking, online shopping and visiting travel websites. When employees access websites for non-business or inappropriate purposes, productivity can be reduced and there is an increased risk that IT assets and users' information could be compromised through malicious software infections. In addition, we found advertising content on four computers which could indicate adware[4] which increases the risk of spyware[5] or malware[6] infections.

We also found that users were not restricted from downloading software. We found that one computer contained 21 computer games. Malicious or unauthorized 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.

The Board Did Not Adopt a Disaster Recovery Plan or Backup Procedures

The Board and Town officials have not developed, adopted and implemented a disaster recovery plan or formal backup procedures. Although certain computers, including those with financial and Justice Court data, are backed up, and some backups are stored locally and others offsite, officials and employees have no guidelines to minimize the loss of equipment or how to implement data recovery

[4] Adware automatically displays or downloads advertising material.

[5] Spyware enables users to obtain covert information about other users' computer activities by transmitting data covertly from their hard drives.

[6] Malware programs are specifically designed to harm computers and data.

in the event of a disaster. Further, Town officials do not have a regular method in place for testing backups. 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.

The Board Did Not Adopt 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 not aware of this requirement. As a result, if PPSI is compromised, officials may not understand or fulfill the Town's legal obligation for notifying 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. By not providing IT security training there is increased risk that users will not understand their responsibilities, putting the data and computer resources at greater risk for unauthorized access, misuse or abuse.

What Do We Recommend?

The Board and Town officials should:

1. Develop, adopt and implement a written acceptable use policy.

2. Design and implement procedures and controls to restrict access to websites and prevent users from installing software.

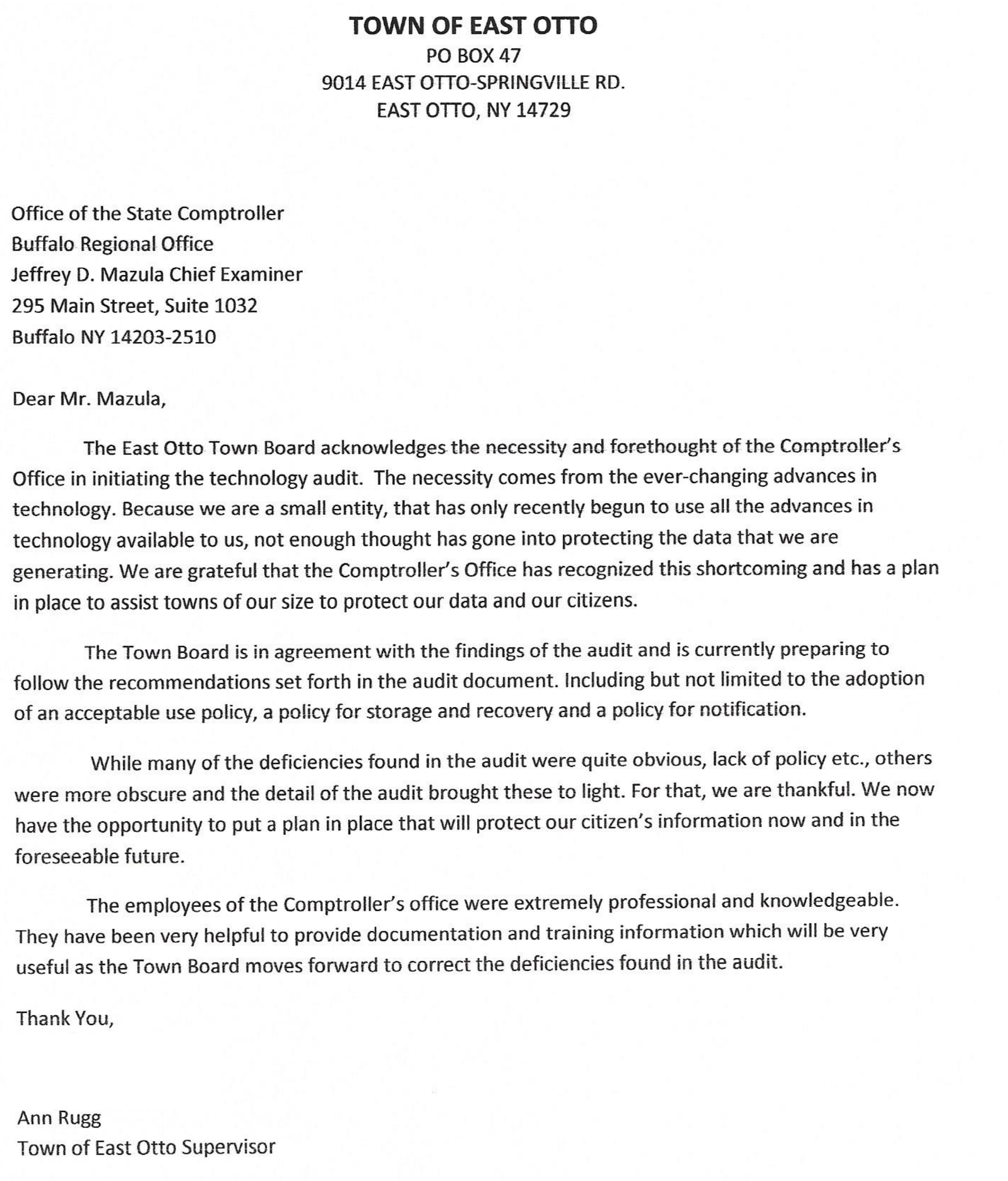
3. Ensure non-work related software programs are uninstalled from Town computers.

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

5. Develop, adopt and implement a written breach notification policy.

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

Appendix A: Response From Town Officials



TOWN OF EAST OTTO
PO BOX 47
9014 EAST OTTO-SPRINGVILLE RD.
EAST OTTO, NY 14729

Office of the State Comptroller
Buffalo Regional Office
Jeffrey D. Mazula Chief Examiner
295 Main Street, Suite 1032
Buffalo NY 14203-2510

Dear Mr. Mazula,

The East Otto Town Board acknowledges the necessity and forethought of the Comptroller's Office in initiating the technology audit. The necessity comes from the ever-changing advances in technology. Because we are a small entity, that has only recently begun to use all the advances in technology available to us, not enough thought has gone into protecting the data that we are generating. We are grateful that the Comptroller's Office has recognized this shortcoming and has a plan in place to assist towns of our size to protect our data and our citizens.

The Town Board is in agreement with the findings of the audit and is currently preparing to follow the recommendations set forth in the audit document. Including but not limited to the adoption of an acceptable use policy, a policy for storage and recovery and a policy for notification.

While many of the deficiencies found in the audit were quite obvious, lack of policy etc., others were more obscure and the detail of the audit brought these to light. For that, we are thankful. We now have the opportunity to put a plan in place that will protect our citizen's information now and in the foreseeable future.

The employees of the Comptroller's office were extremely professional and knowledgeable. They have been very helpful to provide documentation and training information which will be very useful as the Town Board moves forward to correct the deficiencies found in the audit.

Thank You,

Ann Rugg
Town of East Otto 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 to obtain an understanding of the Town's IT environment, internal controls and applicable processes and procedures.
- We examined all six computers to determine whether employees were using computers for personal use or non-work related purposes.
- We performed authenticated scans against all six computers to identify the settings configured. We analyzed the scan results for security weaknesses.
- We interviewed Town officials to determine whether personnel received cybersecurity awareness training.

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 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 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