Town of Hunter

Information Technology

MAY 2019

Contents

Report Highlights

Audit Objective

Determine whether Town officials ensured the Town's information technology (IT) system was adequately secured and protected against unauthorized use, access and loss.

Key Findings

The Board has not:

- Adopted IT policies and procedures for disaster recovery, backups and breach notification.
- Provided IT security awareness training.
- Ensured that IT hardware and software inventories are up-to-date.

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

Key Recommendations

Adopt a disaster recovery plan, backup procedures and a breach notification policy.

Ensure that:

- All personnel receive IT security awareness training.
- IT hardware and software inventories are up-to-date.

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

Background

The Town of Hunter (Town) is located in Greene 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 establishing policies and procedures to safeguard IT assets and provide a secure IT environment.

Town officials contract with an IT consultant for IT services including support, network management and other services.

Quick Facts	
Residents	Approximately 2,700
2018 Appropriations	$3.2 million
Employees	52
Computers in Use	15

Audit Period

January 1, 2017 – August 8, 2018. We extended our scope forward to December 4, 2018 to complete computer testing.

Information Technology

How Should IT Assets Be Safeguarded?

A board should adopt a disaster recovery plan 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. Such a 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. In addition, a board should also establish backup[1] procedures that define the frequency, method and scope of backups and require offsite storage for backup data.

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 with periodic IT security awareness training that explains the proper rules of behavior for using IT systems and data and communicate the policies and procedures to be followed. Security awareness training communicates IT security expectations to employees, helps individuals recognize security concerns and react appropriately and helps ensure employees understand their individual roles and responsibilities.

Town officials should maintain detailed, up-to-date inventory records for all computer hardware and software. The information should include a description of the item (make, model and serial number), the name of the employee to whom the equipment is assigned, 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 computer(s) on which the software is installed and licensing information.

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. While the Town has a system to backup the networked computers, the Board did not assign personnel to switch the backup tapes and store them offsite. Without this manual process, only one generation of backups is kept and stored at the Town. If a disaster occurs, the backup would likely be compromised as well. In addition, without a disaster recovery plan, all responsible parties may not be aware of what they should do, where they should go, or how they will resume business after a disruptive event.

---

1 A backup is a copy of electronic information for use if there is loss or damage to the original.

2 Section 208

The Board Did Not Adopt a Breach Notification Policy

The Board has not developed, adopted and implemented a breach notification policy or local law because it was not aware of this requirement. The Town maintains personal, private and sensitive information (PPSI) in the regular course of its operations; however, if a breach were to occur, 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 the policies and how they could help protect IT assets and computerized data. The IT Consultant was not aware that the Town adopted policies for the use of computers, Internet and email that the employees should be trained on. 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.

Town Officials Did Not Maintain an Inventory of IT Hardware or Software

The IT Consultant or Town officials did not maintain an up-to-date inventory of hardware or software. A Town employee responsible for tracking assets has a list of computers; however, it is not up-to-date because she was not kept up-to-date on changes made. The IT Consultant stated that all of the Town's computers were networked except for one. However, we found five additional standalone workstations in use.

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. In addition, there is an increased risk that loss, theft or misuse of IT assets can occur and that unauthorized devices and software can be easily introduced, putting the Town's data at risk.

What Do We Recommend?

The Board should:

1. Develop, adopt and implement a disaster recovery plan, formal backup procedures, and a breach notification policy or local law.

2. Assign personnel to switch the backup tapes and store them offsite.

3. Ensure all personnel periodically receive IT security awareness training.

4. Ensure that IT hardware and software inventories are up-to-date.

TOWN OF HUNTER
PO BOX 70
TANNERSVILLE, NY 12485
518/589-6150 ext 300

Office of the NYS Comptroller
Newburgh Regional Office
33 Airport Center Drive, Suite 103
New Windsor, NY 12553

May 14, 2019

To Whom it may concern:

The Town of Hunter is in receipt of the preliminary draft findings of an audit that examined our town for the period ending 2017/2018.

The report has brought IT weaknesses to light and we are in agreement that they need to be addressed. We have taken steps and will continue to rectify matters going forward.

Thank you,

DARYL LEGG,
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 and determine whether personnel received IT security awareness training.

- We inquired about IT related policies and procedures and reviewed written policies to obtain an understanding of controls over IT assets and operations.

Our audit also examined the adequacy of certain IT 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.

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 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/pubs/cyber-security-guide.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

NEWBURGH REGIONAL OFFICE – Tenneh Blamah, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties

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