REPORT OF EXAMINATION | 2018M-224

Town of Queensbury

Information Technology

MARCH 2019

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

Contents

Report Highlights

Town of Queensbury

Audit Objective

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

Key Findings

Town officials have not:

- Implemented comprehensive procedures for managing, limiting, securing and monitoring user access.
- Monitored compliance with the acceptable use policy, or developed a formal disaster recovery plan.

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

Key Recommendations

- Implement strong access controls, in part, by removing or disabling unnecessary local user accounts.
- Enforce the acceptable use policy and adopt a comprehensive disaster recovery plan.

Local officials agreed with our recommendations and indicated they have begun corrective action.

Background

The Town of Queensbury (Town) is located in Warren County.

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

Quick Facts

2018 General Fund Budget	$13.5 million
Residents	27,900
Employees	260
Network Accounts	158

Audit Period

January 1, 2017 - April 11, 2018

Information Technology

The Town relies on its IT system for Internet access, email, maintaining financial data, and maintaining and accessing personal, private or sensitive information (PPSI)[1]. If the IT system is compromised, the results could range from inconvenient to catastrophic and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of a computer 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?

Town officials are responsible for restricting users' access to just those applications, resources and data that are necessary for their day-to-day learning, duties and responsibilities to provide reasonable assurance that computer resources are protected from unauthorized use or modifications. User accounts enable the system to recognize specific users, grant appropriate authorized access rights and provide user accountability by affiliating user accounts with specific users, not sharing user accounts among multiple users and disabling user accounts not assigned to specific individuals.

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. Town officials should implement procedures to monitor compliance with the policy.

In addition, safeguarding IT assets should include Town officials developing and adopting a disaster recovery plan to reconstruct vital operations and services after a disaster. Disasters may include any sudden, catastrophic event that compromises the availability or integrity of an IT system and data. Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, disaster prevention instructions, specific roles of key individuals and precautions needed to maintain or quickly resume operations. Additionally, a disaster recovery plan should include data backup procedures such as ensuring a backup is stored off-site in case the building is destroyed or inaccessible, and periodic backup testing to ensure they will function as expected.

1 PPSI is any information to which unauthorized access, disclosure, modification, destruction, or disruption of access or use could severely impact critical functions, employees, customers or third parties, or citizens of New York in general.

Town Officials Did Not Implement Strong Access Controls

Town officials have not implemented comprehensive procedures for managing, limiting, securing and monitoring user access. We noted inactive user accounts, user accounts that are for nonemployees and user accounts not assigned to a specific individual.

We reviewed the Town's 158 network user accounts[2] and found:

- 18 accounts (11 percent) have not been used in at least six months.
- 8 accounts (5 percent) did not match current employees.
- 63 accounts (40 percent) are not tied to individual users.

We also examined the 16 local user accounts[3] on the five servers[4] and 34 local user accounts on 12 computers we selected for testing. We found that:

- 26 accounts (52 percent) have not been used ranging from two to more than five years.
- 40 accounts (80 percent) are not tied to individual users.

Any unnecessary accounts should be disabled or removed as soon as they are no longer needed to decrease the risk of unauthorized access and potential entry points for attackers to copy, manipulate or delete PPSI. Of particular risk are the accounts of non-employees, because these accounts could potentially be used by individuals for malicious activities. Furthermore, accounts not assigned to specific individuals can prevent Town officials from tracing suspicious activity, presenting difficulties in holding the responsible user accountable for their actions. Consequently, the Town's IT assets and data are at increased risk for loss or misuse.

Town Officials Did Not Enforce the Acceptable Use Policy

The Town has an acceptable computer use policy in place that defines the procedures for computer, Internet and email use. However, Town officials have not designed or implemented procedures to monitor compliance with the policy or determine the amount of employees' personal use.

We tested 19 computers and found one computer where PPSI is exposed. Further, we identified questionable Internet use by 12 other employees including:

2 Network user accounts are those accounts that are stored on a centralized server and can be used to log on to multiple computers on the network.

3 Local user accounts are those accounts that are stored locally on the individual computers and can only be used to log on to the computer in which the account is stored.

4 Two servers are domain controllers which store network user accounts, not local user accounts and therefore there are no local user accounts to examine on those two servers.

visits to social media, online shopping, travel, sports, entertainment, personal email and personal financial institution websites, and performed other Internet research and browsing of a personal nature using the Town's IT assets.

Town officials stated that Internet access is granted to users based on job needs, and that user rights, were set up to prevent unacceptable computer usage. Further, they expected that employees were not using computers for personal use. However, while user rights can restrict internet access, it does not prevent personal use and the possibility of exposing PPSI.

By not enforcing the acceptable computer use policy, Town officials are exposing PPSI and other Town data to unauthorized users who may use it for malicious activities. Further, the exposure of PPSI to any unauthorized users would constitute a security breach, which could definitely have negative financial consequences for the individual(s) whose private information was accessed. Such exposure could also have a negative financial impact on the Town, the custodian of this data, if it were found liable for the unauthorized release of confidential information. The occurrence of security breaches also reduces taxpayers' confidence in the Town's ability to safeguard personal information.

The Town Does Not Have a Disaster Recovery Plan

The Board did not develop a formal disaster recovery plan to address potential disasters. Consequently, in the event of a disaster, Town officials have no guidelines to minimize or prevent the loss of equipment and data. This would impact their ability to appropriately recover data and critical operations. Town officials stated that the lack of plan was due to their current priority of transferring the Town's IT services to the Cloud,[5] and a plan would be created with help from their IT vendor. Without a disaster recovery plan, the Town could lose important financial and other data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees or process daily Town clerk functions.

What Do We Recommend?

Town officials should:

1. Implement procedures to evaluate all existing network and local user accounts, remove or disable any deemed unnecessary. Accounts should be periodically reviewed to determine whether they are appropriate and necessary.

2. Enforce the acceptable use policy, including ensuring that all PPSI is not exposed on user computers.

3. Develop and adopt a comprehensive disaster recovery plan.

5 The cloud refers to software and services that run on the Internet, instead of locally on the computer.

Appendix A: Response From Town Officials

TOWN OF QUEENSBURY
"Home of Natural Beauty...A Good Place to Live" Settled 1763

3/7/2019

Office of the State Comptroller
Jeffrey P. Leonard, Chief Examiner
One Broad Street Plaza
Glens Falls, New York 12801-4396

RE: Examination Report 2018M – 224 Local Officials' Response

Dear Mr. Leonard:

Please let this letter serve as both Local Officials' Response for Audit 2018M-224 "Town of Queensbury Information Technology".

The Town of Queensbury has implemented your findings as follows:

Recommendation 1: Implement procedures to evaluate all existing network and local user accounts, remove or disable any deemed unnecessary. Accounts should be periodically reviewed to determine whether they are appropriate and necessary.

Town officials did not implement and adhere to strong security controls. Since that time Written Information Security Policy (WISP) is being implemented (per recommendation) with a periodic review by the IT committee at the Town of Queensbury to review permissions across town users. This review ensures users have access to necessary resources and limits unauthorized permissions to systems or information.

Recommendation 2: Enforce the acceptable use policy, including ensuring that all PPSI is not exposed on user computers.

The Town has an acceptable use policy that is in place currently and has not been actively enforced. With the adoption of the new WISP, the town will actively monitor and remediate infractions through the IT Committee. The town has also committed to additional cybersecurity training and increasing content restrictions to prevent future content and access breaches.

TOWN OF QUEENSBURY

"Home of Natural Beauty...A Good Place to Live" Settled 1763

Recommendation 3: Develop and adopt a comprehensive disaster recovery plan.

The Town did not have an active disaster recovery plan. Since that time, the town has replaced its infrastructure in a fully redundant and scalable solution which allows the town to continue to function in a catastrophic event. This solution is focused on a cloud-based infrastructure allowing the town to function anywhere in the world. The town has worked with its IT vendor to have a plan in place in the event of a system wide failure.

I would like to thank the OSC staff conducting the audit for their courtesy and professionalism.

Sincerely,

John F. Strough
Town 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 objectives[6] and obtain valid audit evidence, our audit procedures included the following:

- We interviewed Town officials, employees and third parties and reviewed the Town's technology use policy to gain an understanding of the Town's IT system and related controls.
- We reviewed the written agreements between the Town and its IT vendor.
- We analyzed and assessed all 158 enabled network user accounts and all 50 enabled local user accounts on 12 computers and five servers on the Town's network. The 12 computers and five servers were selected based on the employee job description and the intended function of the computer and server.
- We examined Internet use on 19 computers connected to the Town's network. The 19 computers were selected based on the employee job description and the intended use of the computer.

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.

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.

6 We also issued a separate audit report, *Town of Queensbury - Water System Cybersecurity (2018M-268)*.

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

GLENS FALLS REGIONAL OFFICE – Jeffrey P. Leonard, Chief Examiner

One Broad Street Plaza • Glens Falls, New York 12801-4396

Tel (518) 793-0057 • Fax (518) 793-5797 • Email: Muni-GlensFalls@osc.ny.gov

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington counties

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