REPORT OF EXAMINATION | 2018M-268

Town of Queensbury

Water System Cybersecurity

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 adequately safeguard electronic access to the Town's water system.

Key Findings

- Water officials have not implemented comprehensive procedures for managing, limiting, securing and monitoring user access.
- Water plant personnel have not been provided with job-specific cybersecurity awareness training.
- Water officials did not prevent or monitor public disclosure of information on the Town's water system.

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

Key Recommendations

- Implement strong access controls.
- Provide cybersecurity awareness training to Water plant employees.
- Prohibit the public disclosure of sensitive water system information.

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. The Water Superintendent is responsible for managing the day-to-day operations of the water department.

The Town maintains computer-based systems to control and monitor water flows, levels, pressure and quality characteristics. Officials contract with a third-party vendor to manage the Town's water system IT components (e.g., computers and network devices). Officials also contract with another third-party vendor to manage the system's operational technology components.

Quick Facts	
Residents	27,900
2018 Water Fund Budget	$4.4 million
Water Customers	9,000
Avg. Daily Potable Water Production	4.5 million gallons

Audit Period

January 1, 2017 - April 11, 2018

Water System Cybersecurity

How Should Water Systems Be Protected?

A disruption to the Town's water system could range from a minor inconvenience to serious consequences relating to the health of both personnel and water customers. The Town and Water Plant officials can minimize the risk of disruptions to the Town's water system by establishing strong access controls to the Town's water system; providing annual cybersecurity awareness training to all personnel; prohibiting vendors from disclosing information about the Town's system; periodically reviewing publicly available content for information that could jeopardize the water system; and adopting and enforcing appropriate IT policies and procedures.

Water Officials Did Not Implement Strong Access Controls

Water officials have not implemented comprehensive procedures for managing, limiting, securing and monitoring user access. We noted inactive user accounts and user accounts not assigned to a specific individual on the Town's water system.

We reviewed 13 local user accounts on the SCADA[1] server and found:

- Seven accounts (54 percent) have not been used to log on ranging from six months to more than three years.
- Four accounts have never been logged on to.
- 11 accounts are not tied to individual users and/or are shared accounts.

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. 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 water system assets and data are at increased risk for unauthorized access, loss or misuse.

Personnel Have Not Received Cybersecurity Awareness Training

Water plant personnel have not been provided with job-specific cybersecurity awareness training. The Water Superintendent stated that his employees are provided with training to learn how to keep the water safe, however, no cybersecurity awareness training was provided.

1 Supervisory control and data acquisition (SCADA) is a software system with hardware elements that allows industrial organizations to monitor and/or control industrial processes locally or at remote locations.

Without cybersecurity awareness training, water plant personnel may not be prepared to recognize and appropriately respond to suspicious water system activity. Unauthorized access could go undetected allowing a malicious individual the opportunity to modify water data, which could cause operators to take actions based on inaccurate information. Alternatively, a malicious user could inappropriately modify device settings causing motors to turn on or off or valves to open or close or chemical feeds to increase or decrease. This could ultimately lead to water shortages, losses, flooding or contamination.

Water Officials Do Not Sufficiently Prevent or Monitor for Public Disclosure of Town Water System Information

Water officials do not prohibit its third-party vendors from disclosing information about the Town's water systems. The service level agreements between the Town and its vendors do not contain terms specific to information disclosure, and officials do not periodically monitor publicly available content for inappropriate disclosure. We performed a limited search for publicly available information about the Town's water systems and provided the results of inappropriately disclosed information to Town officials.

Town officials were unaware that its third-party vendor was disclosing information about the Town's water system. Individuals with malicious intent commonly search the Internet for system details while planning their attacks. Exposing such details unnecessarily provides information to these potential attackers, who could then formulate more focused and effective attacks against the Town's water system.

Officials Have Inadequate IT Policies and Procedures

There are no written policies, procedures, standards or guidelines related to the industrial control system cybersecurity. This includes the use of USB drives, personal devices and other mobile storage devices within the water control system network. Also, job duties do not specify security roles and responsibilities for water personnel to ensure users are aware of and understand what is expected of them to maintain the security of the water control system.

The Water Superintendent stated that the Town is waiting for State mandates and governance from the Department of Homeland Security before creating and implementing written policies and procedures. Not having written guidance for employees to follow could lead to unauthorized access, embedded malicious code, or otherwise disrupt or compromise the Town's water system.

What Do We Recommend?

Water 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. Provide cybersecurity awareness training to Water employees.
3. Ensure that water system service level agreements include terms that prohibit vendors from disclosing information about the Town's water systems.
4. Work with vendors and applicable organizations to remove information that was inappropriately disclosed publicly.
5. Periodically review publicly available content for information that could jeopardize the Town's water system and ensure it is removed from public view.
6. Adopt and implement relevant policies and procedures that address industrial control system cybersecurity.
7. Ensure users roles and responsibilities in regards to maintaining the security of the Town's water systems are documented and users are aware of them.

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 – 268 Local Officials' Response

Dear Mr. Leonard:

Please let this letter serve as both Local Officials' Response for Audit 2018M-268 "Town of Queensbury Water System Cybersecurity".

The Town of Queensbury Water Department 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: Provide cybersecurity awareness training to Water Plant Employees.

The Town has implemented an employee training program to ensure initial and continuing training of all employees including Water Department employees.

Recommendation 3: Ensure that water system service level agreements include terms that prohibit vendors from disclosing information about the Town's water systems.

The Town will monitor the information made available to the public more closely. The Town has decided to provide limited disclosure of confidential information available in public facing forums and systems pursuant to New York State Public Officers Law, Article 6, Section 87, Sub-section 2. The town will ensure that contracts are reviewed to limit disclosure only to required information.

742 Bay Road ♦ Queensbury, NY 12804 ♦ Phone: 518-761-8201 ♦ www.queensbury.net

Recommendation 4: Work with vendors and applicable organizations to remove information that was inappropriately disclosed publicly.

The Town will monitor the information made available to the public more closely. The Town has decided to provide limited disclosure of confidential information available in public facing forums and systems pursuant to New York State Public Officers Law, Article 6, Section 87, Sub-section 2.

Recommendation 5: Periodically review publicly available content for information that could jeopardize the Town's water system and ensure it is removed from public view.

The Town will monitor the information made available to the public more closely. The Town has decided to provide limited disclosure of confidential information available in public facing forums and systems pursuant to New York State Public Officers Law, Article 6, Section 87, Sub-section 2.

Recommendation 6: Adopt and implement relevant policies and procedures that address industrial control system cybersecurity.

The town is continuing to enhance its security policy by limiting access to network and domain devices to named users only. With the adoption of the new WISP, the town has implemented (per recommendation) with a periodic review by the IT committee to review permissions across town users.

Recommendation 7: Ensure users roles and responsibilities in regards to maintaining the security of the Town's water systems are documented and users are aware of them.

The Town has an acceptable use 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 breaches.

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

Sincerely,

John F. Stróugh
Town Supervisor

742 Bay Road ♦ Queensbury, NY 12804 ♦ Phone: 518-761-8201 ♦ www.queensbury.net

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[2] and obtain valid audit evidence, our audit procedures included the following:

- We interviewed Water Plant officials, employees and third parties to gain an understanding of the Town's water system and related cybersecurity controls and procedures.
- We reviewed the written agreements between the Town and its third-party IT vendors.
- We performed Internet searches for publicly available information about the Town's water systems.
- We performed a walk-though of the water plant to obtain an in-depth understanding of the system's functionalities.
- We examined local user accounts on the water system server to determine if weaknesses in user account management and access controls existed.

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.

2 We also issued a seperate audit report, *Town of Quensbury - Information Technology (2018M-224)*.

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