REPORT OF EXAMINATION | 2018M-152

City of Binghamton

Water System Cybersecurity

NOVEMBER 2018

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

Contents

Report Highlights

City of Binghamton

Audit Objective

Determine whether City officials adequately safeguarded electronic access to the water system.

Key Findings

City officials did not:

- Adequately safeguard the electronic access to the water system.
- Implement a formal process to stay updated on system cybersecurity threats.
- Prevent or monitor public disclosure of information that could jeopardize the water system.
- Provide staff with cybersecurity awareness training.

In addition, sensitive information technology (IT) control weaknesses were communicated confidentially to City officials.

Key Recommendations

- Establish a process for receiving and assessing system cybersecurity alerts.
- Adopt policies and procedures to better safeguard the water system.
- Prohibit the disclosure of information that can jeopardize the system and monitor for and remove such publicly shared information.
- Provide cybersecurity awareness training to personnel.
- Address the confidentially communicated IT recommendations.

District officials generally agreed with our recommendations and have initiated or indicated they planned to initiate corrective action. Appendix B includes our comment on an issue raised in the District's response letter.

Background

The City of Binghamton (City) is located within Broome County. The elected seven-member Common Council (Council) is responsible for managing City operations. The Water and Sewer Superintendent (Superintendent) is responsible for overseeing and managing day-to-day water operations.

The City maintains a computer-based system that controls and monitors water flows, levels, pressure and quality characteristics such as pH, temperature and turbidity. The water filtration plant supervisor is responsible for overseeing this system. The IT Manager is responsible for managing the networking devices and the internet connection. The City relies on two service providers for IT support on an as-needed basis.

Quick Facts	
Residents	47,400
Water Customers	13,740
2018 Water Fund Appropriations	$7.4 million
Water Plant Employees	11
Gallons of Water Treated Daily	4.5 million

Audit Period

January 1, 2017 – May 7, 2018

Water System Cybersecurity

How Should Water Systems Be Protected?

A disruption to a city's water system could range from a minor inconvenience to serious consequences relating to the health of personnel and water customers. A city's governing board, IT manager and water plant officials can minimize the risk of disruptions to the water system by establishing a process for receiving and assessing system cybersecurity alerts, adopting and enforcing appropriate IT policies and procedures, periodically reviewing publicly available content for information that could jeopardize the system and providing cybersecurity awareness training to all personnel at least annually.

In addition, New York State Public Health Law (Public Health Law)[1], which was updated on December 31, 2016, required all community water systems that serve more than 3,300 people to prepare and file an updated water supply emergency response plan that includes a vulnerability analysis assessment to a cyberattack with the New York State Department of Health (NYSDOH) by January 1, 2018.

Officials Did Not Assess Cybersecurity Threats

The Superintendent did not establish a formal process for staying current on system cybersecurity threats. Water plant officials do not receive alerts to such threats from key sources, including the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[2] or the Water Information Sharing and Analysis Center (WaterISAC).[3] The Superintendent told us that he relies upon a former employee to occasionally provide cybersecurity threat information. However, this process is unreliable because this former employee may not be familiar with the current water system environment and the information about threats is not regularly provided.

Further, as of May 2018, the City was not in compliance with Public Health Law to protect drinking water. Although the City's emergency response plan was updated and submitted in a timely manner, the vulnerability assessment was not completed until April 2018 and not submitted until August 2018. Before this time, the most recent emergency response plan and vulnerability assessment was submitted in January 2013.

Our review of these documents disclosed several assertions within them that conflicted with the current observed conditions at the water plant. Water plant

1 New York State Public Health Law, Section 1125

2 ICS-CERT provides timely advisories and alerts on information about current security issues and vulnerabilities and notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.

3 WaterISAC keeps drinking water and wastewater managers informed about potential threats and risks to the nation's water infrastructure from all hazards, such as intentional contamination, terrorism and cybercrime and to provide knowledge about response, mitigation and resilience.

officials were unaware of the importance of updating these documents annually or when significant system upgrades are made.

Because officials do not have a process in place to stay updated on cybersecurity threats and ensure that updates to the emergency response plan and vulnerability assessment are made in a timely manner, they could have a false sense of security and lack of awareness of current cybersecurity risks since new cybersecurity threats are continuously appearing and water system technology is rapidly changing.

IT Policies and Procedures Are Inadequate

Water plant officials do not adequately monitor and enforce the restrictions defined in the City's technology use policy (policy), which has not been updated since 2008. The policy includes computer and internet use restrictions such as not allowing non-City licensed software to be installed on computers.

Although we did not find any inappropriate internet use, unnecessary software was installed on all three computers connected to the water system network. In addition, officials did not have any policies in place governing backups, patch management, user account and permissions management or the review of system logs. As a result, water system data is not backed up and patches and updates are not installed in a timely manner. In addition, unnecessary user accounts and permissions were found on all water system computers and software and officials did not regularly review the water system software activity logs.

As a result, officials may find it timely and costly to recreate the water system's configuration and the real-time observation of the processes would not be available during the reconfiguration. Vulnerabilities associated with unpatched software are well-known and there is information freely available on the Internet to help malicious users exploit some of these vulnerabilities. This could lead to unauthorized access or disruption to the water system. Unnecessary accounts and permissions increase the risk of unauthorized access because any account is a potential entry point for attackers. By not regularly reviewing the water system software activity logs, unauthorized access can go undetected allowing greater damage to occur.

Officials Do Not Sufficiently Monitor Website Content

City and water plant officials do not periodically review publicly available content included on the Internet for inappropriate disclosure of water system information. In the 2013 vulnerability assessment, water plant officials recognized the risk associated with information publicly disclosed on the Internet, but did not have a remediation plan.

We searched the Internet in April 2018 to determine whether there was any inappropriate public information about the water system and found that content, which officials realized should have been deleted in 2013 or earlier, was still available as was other system information posted by vendors.

The IT Manager told us that water plant officials are responsible for the content posted on the water department webpage. However, Water officials were under the impression that the IT department handled webpage content. In May 2018, City officials initiated steps to remove some of this information.

When inappropriately disclosed water system information is publicly available, Individuals with malicious intent can search the Internet for system details while planning attacks. Exposing such details unnecessarily provides information to these potential attackers, who could then formulate more focused and effective attacks against the water system.

Personnel Did Not Receive Cybersecurity Awareness Training

The Superintendent did not provide water plant personnel with job-specific cybersecurity awareness training. Without cybersecurity awareness training, personnel may not be prepared to recognize and appropriately respond to suspicious system activity.

As a result, 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, valves to open or close or chemical feeds to increase or decrease. This could ultimately lead to water shortages, losses, flooding or contamination. City officials told us they are preparing City-wide cybersecurity training.

What Do We Recommend?

The Superintendent should:

1. Establish and implement a process for receiving and assessing water system cybersecurity alerts.
2. Ensure job-specific cybersecurity awareness training is provided to all water plant personnel at least annually.

Water plant officials should:

3. Continue to update the water system’s emergency response plan and complete and submit the cybersecurity vulnerability assessment to NYSDOH as soon as possible.

The Council should work with the Superintendent and IT Manager to:

4. Adopt and enforce policies and procedures that adequately address areas such as, but not limited to, physical security, software installations, backup data, patch management, user account and permission management and review of system logs.

5. Adopt and enforce a policy that prohibits disclosing information about the water system on the City's public website.

6. Include terms in service level agreements in future water system related contracts to prohibit vendors from disclosing information about the City's water system.

Appendix A: Response From City Officials

OFFICE OF THE MAYOR

Richard C. David, Mayor
Jared M. Kraham, Executive Assistant
Donna Ferranti, Secretary

November 21, 2018

Ann Singer, Chief Examiner
New York State Office of State Comptroller
Binghamton Regional Office
44 Hawley Street, Room 1702
Binghamton, NY 13901

Subject: City of Water System Cybersecurity Audit Response & Corrective Action Plan
Audit Report #: 2018M-152

The City of Binghamton works diligently to ensure that our Water System is operated with the health and security of our customers as its top priority. It should be noted, that the City Water Department has not been the target of any successful cyber-attacks to date.

The City appreciates the efforts of the Office of the State Comptroller in performing this audit and their recommendations to improve our ability to resist cyber-attacks on our Water System.

The City of Binghamton is in agreement with the findings of the audit and has begun to address the recommendations of the audit. See Corrective Action Plan below.

Audit Recommendation# 1:
Establish and implement a process for receiving and assessing water system cybersecurity alerts.

Implementation Plan:
The City has and will maintain a subscription to WaterISAC. Key staff in the Water Department and IT Department are receiving emails detailing security threats.

Implementation Date:
July 2018

Person Responsible for Implementation:
Lori Clift, Information Technology Manager
Joseph M Yannuzzi, Superintendent Water / Sewer Department

CITY HALL ▪ 38 HAWLEY STREET ▪ BINGHAMTON, NY 13901 ▪ WWW.BINGHAMTON-NY.GOV
PH: (607) 772-7001 ▪ FX: (607) 772-7079

Audit Recommendation# 2:
Ensure job-specific cybersecurity awareness training is provided to all water plant personnel at least annually.

Implementation Plan:
The City has implemented a cybersecurity training requirement for all employees who use computers. A basic online cybersecurity training class has been or will be taken by employees. Additional cybersecurity training classes will be setup for water department employees that is job specific.

Implementation Date:
Basic cybersecurity training: July- November 2018
Job specific cybersecurity training: no later than March 1, 2019

Person Responsible for Implementation:
Joseph M Yannuzzi, Superintendent Water / Sewer Department
Lori Clift, Information Technology Manager

Audit Recommendation# 3:
Continue to update the water system's emergency response plan and complete and submit the cybersecurity vulnerability assessment to NYSDOH as soon as possible.

Implementation Plan:
Working with both the Broome County Health Department and [redacted] the VA recommendations have been completed as of August 10th 2018. Both VA AND ERP have been submitted and accepted as complete.

See Note 1 Page 10

Implementation Date:
August 10th 2018 was the physical submission to the Broome County Health Department
Letter of acceptance and approval written October 18th 2018

Person Responsible for Implementation:
Joseph M Yannuzzi, Superintendent Water / Sewer Department
Jeffrey A Kruger, Supervisor Water Filtration Plant

Audit Recommendation# 4:
Adopt and enforce policies and procedures that adequately address areas such as, but not limited to, physical security, software installations, backup data, patch management, user account and permission management and review of system logs.

Implementation Plan:
Update and create policies in accordance with NYS OSC IT Governance Publication. Policy templates were created in April 2018 and are being modified to meet the City's specifications. Once the policies are completed, they will be reviewed by the Mayor, Personnel Director and Corporation Counsel and then distributed to all employees. Each employee will be required to acknowledge receipt of policies. Policies will be reviewed/updated on an annual basis. Policies will be stored in a location accessible to all employees.

Implementation Date:
All policies will be completed and distributed to employees by June 1, 2019

Person Responsible for Implementation:
Lori Clift, Information Technology Manager

Audit Recommendation# 5:
Adopt and enforce a policy that prohibits disclosing information about the water system on the City's public website.

Implementation Plan:
Immediate action was taken to remove the [redacted] tour video that was posted on our website prior to 2014, which OSC identified as a significant concern.

The City will create and distribute a policy detailing what is and is not acceptable information to post on the City's public website. Meetings will be held to discuss policy with all employees who maintain website. Employees will be required to acknowledge receipt of policy. Policy will be reviewed and updated annually. A meeting will be held annually with employees who maintain the website to review the policy. Information Technology staff will review the website on a monthly basis to verify that no restricted information is being posted.

Implementation Date:
Removal of [redacted] tour video – May 2018
Creation of policy and employee education to be completed by February 1, 2019

Person Responsible for Implementation:
Lori Clift, Information Technology Manager

Audit Recommendation# 6:
Include terms in service level agreements in future water system related contracts to prohibit vendors from disclosing information about the City's water system.

Implementation Plan:
The Engineering Department will add language to contract template and Corporation Counsel will add language to vendor created contracts prohibiting vendors from disclosing information about the City's water system.

Implementation Date:
February 1, 2019

Person Responsible for Implementation:
Ray Standish, City Engineer
Ken Frank, Corporation Counsel

Sincerely,

Richard C. David,
Mayor

Appendix B: OSC Comment on the City's Response

Note 1

City officials are referring to the vulnerability assessment (VA) and emergency response plan (ERP).

Appendix C: 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 City and water plant officials and reviewed the technology use policy to gain an understanding of the water system and related cybersecurity controls and procedures.
- We reviewed the most recent emergency response plan and vulnerability assessment to determine whether it complied with Public Health Law.
- We analyzed and assessed the activity logs, local user accounts and the security settings applied to those accounts on all three computers connected to the water system network.
- We examined Internet use and operating and application software installed on all three computers connected to the water system network.
- We performed Internet searches for publicly available information about the water system.

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 City 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 Council to make the CAP available for public review in the Clerk's office.

Appendix D: 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

BINGHAMTON REGIONAL OFFICE – Ann C. Singer, Chief Examiner

State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417

Tel (607) 721-8306 • Fax (607) 721-8313 • Email: Muni-Binghamton@osc.ny.gov

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins counties

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