DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2019M-173

City of Syracuse

Water System Cybersecurity

JUNE 2020

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

Contents

Report Highlights

City of Syracuse

Audit Objective

Determine whether City officials properly implemented information technology (IT) security controls to safeguard water system operations against unauthorized access or disruption.

Key Findings

- Network and local user accounts were not properly managed.
- Officials did not establish a process for staying current on water system cybersecurity threats.
- The City did not have service level agreements (SLAs) with its IT vendors.

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

Key Recommendations

- Properly manage network and local user accounts, including disabling unneeded accounts in a timely manner.
- Establish a process for staying current on water system cybersecurity threats.
- Ensure that all IT services are provided based on a formal service level agreement.

City officials generally agreed with our recommendations and indicated they plan to initiate corrective action.

Background

The City of Syracuse (City) is located in Onondaga County. The Common Council (Council) had 10 elected members and was responsible for overseeing the City's operations and finances, including establishing policies and procedures to safeguard water operations.

The Water Commissioner (Commissioner) was responsible for overseeing and managing the water system's day-to-day operations. The City's IT Director was responsible for overseeing and managing the City's IT operations.

A technician in the City's IT Department, under the direction of the Commissioner and in coordination with the IT Director, was responsible for managing the Water Department's (Department's) IT components (e.g., computers and network devices).

Quick Facts	
City Population	145,170
Water Customers	34,645
Water Department Employees	108
Gallons of Water Treated Daily	39 million

Audit Period

July 1, 2017 – May 8, 2019

Water System Cybersecurity

The City's primary water supply is Skaneateles Lake, which is located approximately 20 miles southwest of the City. The City relied on a computer-based water system for monitoring and controlling water flows, levels, pressures and quality characteristics from its water supply, including pH, temperature and turbidity.

The water system had two main software applications,[1] the Water Administration and Skaneateles applications, which resided on two application server computers[2] and were routinely accessed using four user computers. The applications and server and user computers were connected to the City's network,[3] and the Department's access to network resources were managed using two additional server computers.[4] The Department relied on three primary third-party vendors for water system technology support.

The City's water system resembled a traditional computer system that could be affected by cybersecurity vulnerabilities. Officials must protect the water system against cybersecurity threats because a system compromise or disruption could cause water losses, shortages, flooding or contamination that could seriously affect the health of City employees and water consumers.

How Should Officials Manage Access to the Water System?

Computer networks[5] can be accessed by network user accounts, computers can be accessed using local user accounts and applications can be accessed using application user accounts. All of these user accounts identify specific users.

Network user accounts are managed centrally by a server computer and/or domain controller[6] and provide access to resources on a network. Local user accounts are managed individually on each computer and provide access to resources on specific computers. Application user accounts can be managed centrally by an application server and provide access to resources within the application.

---

1 City water personnel also used a third application that was not critical to the continued performance of water operations.

2 A server is a computer equipped with specific programs that provide resources and data to other computers that are connected to the server.

3 These were not the only devices and applications connected to the City's network. Other devices and applications included those used for financial, fire protection, highway maintenance and parks and recreation services and operations.

4 Refer to Appendix B for information on the server and user computers that we reviewed.

5 A group of two or more connected computers

6 A domain controller is the main server computer in the domain (network) that controls or manages all computers within the domain.

To minimize the risk of unauthorized network, computer and application access, officials should actively manage network, local and application user accounts, including their creation, use and dormancy, and regularly review them to ensure they are still needed. When employees leave City employment or when user accounts are otherwise no longer needed, officials should ensure that these accounts are disabled in a timely manner.

A shared account is a network, local or application user account with a username and password that is shared among two or more people. Because shared accounts are not assigned to a single user, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user. To help ensure individual accountability, all users should have and use their own user account to gain access to a network, computer or application.

Officials Did Not Disable All Unneeded User Accounts

We reviewed all 1,055 network user accounts on the City's network, of which 168 were generic accounts.[7] We also examined all 16 application user accounts in the Water Administration and Skaneateles applications and 12 local user accounts on the two application server computers (three local accounts) and four user computers (nine local accounts).[8] While we did not find any unneeded application user accounts, we found discrepancies related to network user accounts and local user accounts, as follows:

Unneeded Network User Accounts – We found 10 unneeded accounts on the City's network and another 17 accounts that might have been unneeded. Four of the unneeded accounts belonged to former employees. City officials told us they disabled these four accounts during our fieldwork.

The remaining six unneeded and 17 questionable accounts were generic accounts. When we discussed these accounts with officials, they told us they disabled the six unneeded accounts during our fieldwork. They also told us they would investigate the remaining questionable accounts and disable them if necessary.

Generic user accounts can be difficult to manage, including identifying those that should be disabled, because it may not always be clear exactly who uses the accounts and whether the access is still needed.

7 Network user accounts are used to access computers and other resources on a network. Generic accounts are used by certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs. For example, generic accounts can be used for training purposes or as a generic email account, such as a service helpdesk account. Generic accounts that are not related to specific system needs should be routinely evaluated and disabled, if necessary.

8 Application user accounts are used to access specific applications, and local user accounts are used to access files and software programs on a specific server or user computer.

Unneeded Local User Accounts – We found four unneeded local user accounts on two user computers that had not been disabled despite no longer being needed. These accounts were previously created by City employees who worked for the City's IT Department.

Although two of the four accounts had not been used for more than two years, officials did not detect them as being unneeded because the process they followed to monitor user accounts was limited to individual network user accounts only. It did not include monitoring generic network user accounts and local user accounts on server and user computers.

Unneeded user accounts increase the risk of water system compromise or disruption because any account on a network or computer is a potential entry point for attackers. Of particular risk are the accounts of former employees because these accounts could potentially be used by those individuals or others for malicious activities. In addition, because the City did not have formal procedures for regularly reviewing generic network user accounts and local user accounts on server and user computers, its unused accounts were not being adequately managed.

Some City Employees Shared User Accounts

While users accessed the Skaneateles application using their own application user accounts, they generally accessed the Water Administration application using one shared application user account. Officials told us that staff did this because the Water Administration application must be continuously monitored, and officials also felt it was impractical for users to repeatedly log on and off this application using different user accounts. Officials believed this practice did not significantly diminish accountability because only two users typically accessed the application at any given time.

In addition, IT personnel used one of seven shared administrative accounts to update or perform maintenance on two servers and four user computers. Officials told us they did not have a process for reviewing local user accounts, including those that were shared.

Although only a limited number of users might be sharing access credentials, if problems occurred officials could have difficulty holding users accountable and taking disciplinary action because any user could blame their activity on another.

Why Should Officials Be Aware of Water System Cybersecurity Threats?

To provide effective IT governance and minimize the risk of water system compromise or disruption, the City's governing board should ensure a process is established for staying current on water system cybersecurity threats.

A cybersecurity threat model process should include procedures for regularly reviewing relevant cybersecurity alerts and advisories available from reputable sources, such as the Water Information Sharing and Analysis Center (WaterISAC) and the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

In addition, New York State Public Health Law (Public Health Law)[9] requires emergency response plans and vulnerability assessments of all community water systems that serve more than 3,300 people. These plans and assessments must be prepared, updated at least annually and submitted to the New York State Department of Health every five years. The Public Health Law was updated on December 31, 2016 to further require a cybersecurity assessment be performed and results incorporated into the next emergency response plan and vulnerability assessment update.

Officials Did Not Stay Current on Water System Cybersecurity Threats

Officials did not establish a process for staying current on water system cybersecurity threats. City water personnel do not receive alerts of such threats from key sources such as WaterISAC or ICS-CERT. In addition, while officials began updating the City's emergency response plan and vulnerability assessment during our audit fieldwork, the plan and assessment was last updated in March 2014, five years prior to our audit.

The City contracted with a third-party vendor to perform a cybersecurity assessment in accordance with the updated Public Health Law, and officials received a report detailing the assessment results and recommendations in January 2018. However, as of May 2019, officials were still in the process of establishing a plan to address the vendors' recommendations. Also, they had not incorporated the results into the City's emergency response plan and vulnerability assessment.

The Commissioner told us he relied on third-party vendors to inform him of any cybersecurity threats affecting the City's water system. However, there were no service level agreements requiring the City's third-party vendors to provide this information.[10]

The Commissioner also told us he was unaware that, according to the Public Health Law, the City's plan and assessment needed to be annually updated. Also, he was unaware that, according to the same law, the cybersecurity assessment results needed to be incorporated into the plan and assessment as well.

9 New York State Public Health Law, Section 1125

10 Refer to the "Officials Did Not Maintain Service Level Agreements with Water System Vendors" section for further information.

Without a formal process in place to stay current on cybersecurity threats, officials cannot ensure they are adequately safeguarding the City's water system against those threats. Because cybersecurity threats are continuously emerging and water system technology is rapidly changing, officials could have a false sense of security or lack awareness of current water system threats and be unprepared in the event of a water system emergency.

Why Should the City Have a Service Level Agreement (SLA) With its IT Service Providers?

To protect the City and avoid potential misunderstandings, officials should have a written SLA between the City and its IT service providers that identifies the City's needs and expectations and specifies the level of service to be provided.

An SLA is different from a traditional written contract in that it establishes comprehensive, measureable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. It provides detailed explanations of the services to be performed by identifying the parties to the contract and defining terminology; duration of the agreement, scope and/or subject limitations; service level objectives and performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval process; and pricing, billing and terms of payment.

The SLA should be reviewed by knowledgeable IT staff, legal counsel, or both, and be periodically reviewed, especially if the IT environment or needs change significantly.

Officials Did Not Maintain Service Level Agreements with Water System Vendors

The City did not have service level agreements with any of the three vendors that provide the primary support for its water system technology. During our audit, we identified confusion regarding responsibilities related to essential tasks for proper maintenance of water system cybersecurity. For example, the IT Director told us that a vendor was responsible for configuring the Water Administration application server, while the vendor told us that his responsibility was limited to configuring the application itself.

Inconsistent understanding of responsibilities often leads to gaps in cybersecurity practices. The failure to perform essential cybersecurity tasks, such as managing user permissions and applying security patches, could leave the City's water system vulnerable to compromise or disruption.

Even if officials and vendor personnel had a strong relationship and a consistent understanding of responsibilities, not having written agreements documenting this understanding may absolve vendors of accountability and leave City officials with little to no recourse should disagreements occur.

What Do We Recommend?

The Commissioner and IT Director should:

1. Ensure all unneeded user accounts are disabled in a timely manner.
2. Revise the process for monitoring user accounts to include generic network user accounts and local user accounts on the City's servers and user computers.
3. Ensure all IT users use their own user account to access the City's computers and applications.
4. Ensure IT personnel use their own designated administrative accounts to install software updates and perform maintenance on computers.
5. Update the City's emergency response plan and vulnerability assessment to include the water system cybersecurity assessment results and submit the plan to the New York State Department of Health in a timely manner.

The Council should:

6. Ensure the Department establishes a process for staying current on water system cybersecurity threats.
7. Adopt written service level agreements with the City's third-party IT vendors. Ensure the agreements define a mutual understanding of the City's needs and expectations and specify vendors' roles and responsibilities.

Appendix A: Response From City Officials

In their response, City officials refer to a page number from the draft report that has changed during processing of the final report.

CITY ADMINISTRATION

CITY OF SYRACUSE, MAYOR BEN WALSH

June 12, 2020

Frank Caliva
Chief Administrative Officer

Rebecca Wilcox, Chief Examiner
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428

VIA Email: Muni-Syracuse@osc.ny.gov

RE: **Syracuse Water System Audit Report**
Audit Report Number: **2019M-173**

Dear Ms. Wilcox:

On behalf of Mayor Ben Walsh thank you for the time, diligence and focus provided by the State Comptroller's Division of Local Government and School Accountability.

We found the referenced audit process very instructional and the recommendations very helpful. As noted below, the City largely agrees with your team's findings and has remediated accordingly.

Please do not hesitate to contact me if additional information about our response is required.

Sincerely,

Frank Caliva

City Administration
203 City Hall
233 E. Washington St.
Syracuse, N.Y. 13202

Office 315 448-8018
Email: fcaliva@syrgov.net

www.syrgov.net

Cc: Mayor Ben Walsh
Corey Driscoll Dunham, Director of Operations
Joseph Awald, Commissioner of Water
David Prowak, Director of Information Technology

City of Syracuse Response to Recommendations

GROWTH. DIVERSITY. OPPORTUNITY FOR ALL.

1. Ensure all unneeded user accounts are disabled in a timely manner

   Response: The detailed findings for this item have all been reviewed and unneeded accounts removed.

2. Revise the process for monitoring user accounts to include generic network user accounts and local user accounts on the City's servers and user computers.

   Response: This concern has largely been addressed, with the few remaining generic accounts having a minimum of privileges. The majority of the generic accounts identified by the audit were accounts used for general departmental mailboxes and service accounts. The audit notes this on page 5 footnote #7. Many of these accounts had complex passwords that were not shared with any users. The City monitors for failed login attempts, so any attempts to exploit these accounts would be reported. Recognizing the concern, I.T will develop alternatives and work to eliminate these remaining generic accounts.

3. Ensure all IT users use their own user account to access the City's computers and applications.

   Response: The findings for this item have been reviewed and communicated to all of I.T. staff. Management will continue to monitor for compliance.

4. Ensure IT personnel use their own designated administrative accounts to install software updates and perform maintenance on computers.

   Response: The detailed findings for this item have been reviewed, communicated with I.T. staff and elevated privileged accounts are available for all I.T. staff that require them. Management will continue to monitor for compliance.

5. Update the City's emergency response plan and vulnerability assessment to include the water system cybersecurity assessment results and submit the plan to the New York State Department of Health in a timely manner.

   Response: The ERP and vulnerability assessments have been completed. The Self Certification with EAP is also complete. Copies of reports are being sent to the local DOH offices. The Commissioner of Water will ensure ongoing compliance.

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 City officials, employees and third-party vendor personnel to gain an understanding of the City's water system and related cybersecurity controls and how City officials stay current on water system threats.
- We reviewed the City's IT policies and procedures related to protecting the water system to assess their adequacy.
- We reviewed the Department's emergency response plan and vulnerability assessment to determine whether it complied with Public Health Law.
- We used our professional judgment to review a sample of four server and four user computers, out of a total population of 48 server and user computers, primarily used by the Department to access and transmit water data. The server computers included the Water Administration and Skaneateles application server computers, the Department's local server computer and the City's domain controller. The user computers included those used by Department personnel. We reviewed all 1,055 network user accounts on the City's network, 16 application user accounts in the Water Administration and Skaneateles applications and 12 local user accounts on the application servers and user computers to determine whether they were appropriate and necessary.

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 generally accepted government auditing standards (GAGAS). 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.

The Council has the responsibility to initiate corrective action. 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 City Clerk's office.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2018-12/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263196&issued=All

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263206&issued=All

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2020-05/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/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263211&issued=All

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

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/local-government

Local Government and School Accountability Help Line: (866) 321-8503

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner

State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428

Tel (315) 428-4192 • Fax (315) 426-2119 • Email: Muni-Syracuse@osc.ny.gov

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

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