REPORT OF EXAMINATION | 2021M-178

Otego-Unadilla Central School District

Information Technology

MARCH 2022

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

Contents

Report Highlights

Otego-Unadilla Central School District

Audit Objective

Determine whether the Otego-Unadilla Central School District (District) Board and officials ensured District computerized data was safeguarded through training, monitoring user accounts and adopting a written information technology (IT) contingency plan.

Key Findings

The Board and District officials did not ensure computerized data was safeguarded. In addition to sensitive IT control weaknesses that we communicated confidentially to District officials, we found:

- The District had 58 unneeded user accounts.
- Officials did not provide IT security awareness training.
- The Board did not adopt a written IT contingency plan.

Key Recommendations

- Thoroughly review user access on a routine basis and disable any unnecessary network user accounts as soon as they are no longer needed.
- Provide periodic IT security awareness training.
- Develop and adopt a comprehensive written IT contingency plan.

District officials generally agreed with the findings in our report and indicated they plan to initiate corrective action.

Background

The District serves the Towns of Franklin and Sidney in Delaware County and Otego, Unadilla, Laurens, Oneonta and Butternuts in Otsego County.

The District is governed by an elected seven-member Board of Education (Board) responsible for managing and controlling financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer and is responsible for District administration.

The District's Director of Technology (Director) is responsible for managing the District's IT operations and reports to the Superintendent and Board. The District contracts with South Central Regional Information Center (SCRIC) to provide IT services including an assigned IT Coordinator, hardware/software purchases, technical support, monitoring network user accounts and providing IT security awareness training.

Quick Facts	
# of Student Accounts	919
# of Nonstudent Accounts	273
# of Employees	186
SCRIC IT Contract for 2020-21	$769,625

Audit Period

July 1, 2019 – April 23, 2021

Information Technology

How Should the Board and Officials Manage User Accounts?

Network resources include those on networked computers, such as shared folders, and in certain applications, such as an email application. Network user accounts provide access to network resources and should be actively managed to minimize risk of misuse. If not properly managed, network user accounts could be potential entry points for attackers because they could be used to inappropriately access and view personal, private and sensitive information (PPSI),[1] make changes to employee or student records or deny access to electronic information.

To minimize the risk of unauthorized access, officials should actively manage user accounts including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized. When user accounts are no longer needed, they should be disabled in a timely manner. A school district should have written policies and procedures for granting, changing and removing user access to the network. In addition, generic accounts are not linked to individual users and may be needed for certain network services or applications to run properly. For example, generic accounts can be created and used for automated backup or testing processes, training purposes or generic email accounts, such as a service helpdesk account. Officials should routinely evaluate and disable any generic accounts that are not related to a specific need.

We… identified 58 nonstudent network user accounts (21 percent) were unneeded and could be disabled. …

The Board and Officials Did Not Adequately Manage Network User Accounts

The District's Director is responsible for monitoring network user accounts and requesting new, or changes to, the accounts throughout the year as needed. The Director sends requests to create, change or remove a user account to SCRIC employees who would set up, or make changes to, the network user accounts, including generic accounts.

We reviewed all of the District's 273 nonstudent network user accounts and four local user accounts and identified 58 nonstudent network user accounts (21 percent) were unneeded and could be disabled, including 34 generic user accounts and the accounts for 19 former employees. The majority of the unneeded generic accounts were accounts that had not been used in more than six months and officials determined they could be deleted. District officials told us some of the accounts, such as those related to SCRIC services or used for account testing, would not have been analyzed as part of the annual review. Other accounts were part of the annual review and should have been deleted.

1 Personal, private and sensitive information (PPSI) is any information where authorized access, disclosure, modification, destruction or use—or disruption of access or use—could have or cause a severe impact on critical functions, employees, customers, third parties, or other individuals or entities.

While the District has procedures to add or delete user accounts to the network, the Board did not adopt written policies or procedures for granting, changing and removing user access to the network. The Director told us, as a result of many retirements, they did not review the District's network user accounts to determine whether they were needed before the 2020-21 school year began. This review also did not take place prior to our review of these accounts. The Director told us that the unneeded accounts we identified would be disabled or closed.

Unneeded network user accounts can be potential entry points for attackers and could be used to inappropriately access and view student or employee PPSI. This increases the risk that this PPSI could be changed intentionally or unintentionally or used inappropriately.

Why Should the District Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, school district officials should provide periodic IT security awareness training that explains rules of behavior for using the Internet and IT systems and data, and communicates related policies and procedures to all employees. The training should center on, but not limited to, emerging trends such as information theft and social engineering attacks (methods used to deceive users into revealing confidential or sensitive information), computer viruses and other types of malicious software, all of which may result in PPSI compromise. Training programs should be directed at the specific audience (e.g., system users or administrators).

The training should also cover key security concepts such as the dangers of downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected.

> …[D]istrict officials should provide periodic IT security awareness training that explains rules of behavior for using the Internet and IT systems and data. …

District Employees Were Not Provided With IT Security Awareness Training

The District has a policy that requires District officers and employees to receive annual privacy and security awareness training. However, the District does not have a plan in place to provide security awareness training to independent contractors. Further, it did not provide this training to staff in the 2019-20 school year. SCRIC offers online security awareness training, and the Director enrolled the District for this training during 2020-21 with the intent of providing the training on staff development day. However, due to the COVID-19 pandemic, the Board began the school year being fully remote and used all of the District's conference days preparing for online learning. Prior to the completion of our audit, in

October 2021, SCRIC provided security awareness training to District staff and documented their attendance with a sign-in sheet.

Without annual IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise the District's IT assets and security. As a result, data and PPSI are at a greater risk for unauthorized access, misuse or loss.

Why Should the Board Adopt an Information Technology Contingency Plan?

To minimize the risk of data loss or suffering a serious interruption of service, school district officials should establish a comprehensive written IT contingency plan. The plan should address the potential for sudden, unplanned disruptions (e.g., ransomware or other malware attack, inadvertent employee action or fire) that could compromise the network and the availability or integrity of the school district's IT system and data, including its applications and PPSI.

Typically, an IT contingency plan involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions to maintain or quickly resume operations. It should also reference how the school district should back up its computer systems. Backup data should be stored at a secure offsite location, maintained off-network, encrypted and routinely tested to ensure its integrity. The plan should also be periodically tested, shared and updated to ensure key officials understand their roles and responsibilities during an unplanned IT disruption and to address changes in security requirements.

The Board Did Not Adopt an Information Technology Contingency Plan

While SCRIC performs backups of the District's data and SCRIC has its own contingency plan, District officials did not develop an IT contingency plan for the District's IT systems. Although District backups are performed daily and stored at multiple sites − and SCRIC officials told us that backups are periodically restored to ensure data is available and the backup process is working − the Board has not adopted a written contingency plan to address potential disasters. Consequently, in the event of a disaster, officials have no District-specific guidelines to minimize or prevent the loss of equipment and data or to appropriately recover data or resume operations.

The collective challenges that all school districts endured made it clear that they heavily rely on technology to keep educational systems functioning while also keeping PPSI protected and secure. Without an IT contingency plan, the District could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees or process

grades and State aid claims. When we discussed the importance of a contingency plan with officials, the Director stated that prior to reviewing updates to New York State Education Law, he was unaware of the need to have an IT contingency plan. However, officials should have realized the importance of having an IT contingency plan in place. District officials have discussed the need to formulate a written plan.

What Do We Recommend?

The Board should:

1. Adopt written policies or procedures for granting, changing and removing user access to the network

The Director should:

2. Ensure that any unnecessary network user accounts are disabled as soon as they are no longer needed and thoroughly reviews user accounts on a routine basis.

3. Evaluate the District's current procedures and adjust them as needed to ensure unneeded user accounts are disabled in a timely manner.

District officials should ensure that:

4. Periodic IT security awareness training is provided to employees and independent contractors.

The Board and District officials should:

5. Assign specific IT responsibilities while they develop and adopt a comprehensive written IT contingency plan.

Appendix A: Response From District Officials

Unatego Central School
PO BOX 483
2641 STATE HIGHWAY 7
OTEGO, NEW YORK 13825-9795
www.unatego.org
FAX (607) 988 -1039

Dr. David S. Richards
Superintendent of Schools
(607) 988 -5038

Patricia Loker
Business Manager
(607) 988-5038

February 21, 2022

Office of the New York State Comptroller
Ann C. Singer, Chief Examiner
State Office Building, 44 Hawley Street, Suite 1702
Binghamton, New York 13901-4417

Dear Ms. Singer,

The Otego-Unadilla School District is in receipt of the Draft Audit Report *Information Technology* prepared by the Office of the New York State Comptroller. On behalf of the Board of Education and District Administration, we would like to thank the Comptroller's Staff for their professionalism and courtesy in conducting their duties associated with this audit.

Please accept this letter as the Otego-Unadilla Central School District's official audit response for audit 2021M-178. The audit, referenced above, set out to "determine whether the Otego-Unadilla Central School District Board and officials ensured District computerized data was safeguarded through training, monitoring user accounts, and adopting a written information technology (IT) plan." The audit found that the Board and District officials failed to ensure computerized data was always safeguarded. In general, the District agrees with the key findings of the audit.

Key Findings

The Board and District officials did not ensure computerized data was safeguarded. In addition to sensitive IT control weaknesses that we communicated confidentially to District officials, we found:

- The District had 58 unneeded user accounts.
- Officials did not provide IT security awareness training.
- The Board did not adopt a written IT contingency plan.

The audit also made three key recommendations.

Key Recommendations

- Thoroughly review user access on a routine basis and disable any unnecessary network user accounts as soon as they are no longer needed.
- Provide periodic IT security awareness training.
- Develop and adopt a comprehensive IT contingency plan.

The Otego Unadilla Central School District agrees with the recommendations for more frequent review of user access, the necessity to provide periodic IT security awareness training, and the importance of

developing and adopting a comprehensive IT contingency plan and has already taken steps to implement the recommendations. The District's Corrective Action Plan (CAP) will outline changes to policies and procedures that have been and will be implemented. The District CAP will tentatively be approved at the March 7th Board of Education meeting.

On behalf of the Otego-Unadilla Central School District,

Dr. David S. Richards
Superintendent of Schools

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 our audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed the District's IT policies and procedures and interviewed District officials to gain an understanding of the District's IT operations and determine the adequacy of the policies and procedures.
- We reviewed the District's network user accounts and related settings using a specialized audit script. We excluded student network user accounts, as these accounts had more restricted access and are considered lower risk for potential access to computerized data containing PPSI. We reviewed the remaining 273 nonstudent network user accounts and compared these accounts to the active employee list and discussed these accounts with District officials to identify inactive and unused accounts.

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 District 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 Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of GML, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. 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. The CAP should be posted on the District's website for public review.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

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

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/files/local-government/publications/pdf/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

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

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, Tioga, Tompkins counties

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