OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Victor Central School District

Information Technology

Report of Examination

Period Covered:

July 1, 2014 – March 4, 2016

2016M-117

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

July 2016

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help school district officials manage their districts efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as districts' compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving district operations and Board of Education governance. Audits also can identify strategies to reduce district costs and to strengthen controls intended to safeguard district assets.

Following is a report of our audit of the Victor Central School District, entitled Information Technology. This audit was conducted 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.

This audit's results and recommendations are resources for district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

Introduction

Background

The Victor Central School District (District) is located in the Town of Perinton in Monroe County, the Towns of East Bloomfield, Farmington and Victor in Ontario County and the Town of Macedon in Wayne County. The District is governed by the Board of Education (Board), which is composed of seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The District operates five buildings on one campus with approximately 4,360 students and 690 full- and part-time employees. The District's budgeted appropriations for the 2015-16 fiscal year are $64 million, which are funded primarily with State aid, real property taxes and grants.

The District uses network and internet resources to support business operations including online banking and communications. The District also uses the network and internet to maintain financial records, student records and other personal, private and sensitive information. The Director of Computer Services is responsible for directing the day-to-day operations of the technology department and staff. These responsibilities include maintaining computer hardware and software and coordinating the security of the central information systems and network. The District has an inventory of approximately 560 desktops, 1,560 laptops and 160 tablets. The 2015-16 fiscal year information technology (IT) budgeted appropriations are approximately $1 million.

Objective

The objective of our audit was to review IT security. Our audit addressed the following related question:

- Did the District adequately safeguard and secure its computerized data?

Scope and Methodology

We examined the District's IT security for the period July 1, 2014 through March 4, 2016. We expanded our scope to include a review of information classifications performed on December 5, 2013.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are

included in Appendix B of this report. 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.

Comments of District Officials and Corrective Action

The results of our audit and recommendations have been discussed with District officials, and their comments, which appear in Appendix A, have been considered in preparing this report. District officials generally agreed with our findings and indicated they plan to initiate corrective action.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education, 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, with a copy forwarded to 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 Board should make the CAP available for public review in the District Clerk's office.

Information Technology

The District relies on its information technology (IT) system to perform a variety of tasks, including internet access, storing data, email communication, recording financial transactions and reporting to State and federal agencies. Therefore, the District's IT system and the data it holds are valuable resources that need to be protected from unauthorized, inappropriate and wasteful use. Even small disruptions in IT systems can require extensive time and effort to evaluate and repair. The Board and District officials are responsible for designing and implementing policies and procedures to mitigate these risks. Protecting IT assets is especially important as the number of instances of people with malicious intent trying to harm computer networks and/or gain unauthorized access to information through the use of viruses, malware and other types of attacks continues to rise.

The Board and District officials have not implemented appropriate IT policies and procedures related to personal, private and sensitive information (PPSI)[1] classification or data backups. Additionally, the Board has not adopted a sufficient, comprehensive disaster recovery plan. Consequently, IT assets are at risk for unauthorized, inappropriate and wasteful use, and the District could encounter an interruption in services.

PPSI Classification

Information classification is a necessary part of information security management in any organization. A comprehensive PPSI classification policy defines PPSI, explains the entity's reasons for collecting PPSI, and describes specific procedures for the use, access to, storage and disposal of PPSI involved in normal business activities. The policy should also include data classification requirements. All information, whether in printed or electronic form, should be classified and labeled in a consistent manner to ensure data confidentiality, integrity and availability.

The data classification process assigns a level of risk to various types of information, which helps District officials make appropriate decisions about the level of security the data requires. Therefore, it is important that District officials classify information in a consistent manner to determine the level of security each type of data needs.

[1] PPSI is any information which unauthorized access to, or disclosure, modification, destruction or disruption of access or use, could severely impact critical functions, employees, customers or third parties. Private information could include one or more of the following: social security number, driver's license number or non-driver ID, bank account number, credit or debit card numbers and security code, access code/password that permits access to an individual's financial account, or protected student records.

District officials also should conduct an inventory of PPSI stored on all their electronic equipment to account for the confidential data maintained. District officials should update the classification and inventory list on an ongoing basis, as appropriate, to reflect any changes. In the event of a data breach, the proper classification and inventorying of PPSI allows District officials to determine the extent of unauthorized access and take appropriate action.

As part of our previous audit in 2012,[2] we found that District officials had not completed an inventory or classification of PPSI data. District officials provided a corrective action plan to address the weaknesses identified. During the 2013-14 school year, the Director of Computer Services also conducted a comprehensive information classification of all the District's departments, with the assistance of the various department directors and the Superintendent. However, District officials have not updated the PPSI inventory since. District management told us that they filed the department inventories with the records manager.

We spoke to three employees about the classification process that took place in 2013-14. Although they recalled that the classification was done, one employee stated that the department's data management had not changed, another stated that they never saw the final classifications and a third stated that a few changes were instituted.[3] Therefore, District management went through the process of inventorying and classifying the data that each department maintained but did not properly communicate the results to the employees that handled the data. Additionally, District management did not establish, and the Board did not adopt, a PPSI classification policy to explain what each of the classifications mean. The data was classified as either low, moderate or high, but standards were not developed guiding employees on how each level of data should be handled and secured. Therefore, District staff were unable to act on the information contained in the inventory classification.

As a result, employees are still unaware of the extent that PPSI resides in the electronic equipment that they use on a regular basis and the classifications assigned to the data that they maintain. Consequently, they cannot protect the data as intended. Unless District officials classify the data they maintain, set appropriate security levels for PPSI and update the classification and inventory on an ongoing basis, there is an increased risk that PPSI, such as employee and student

[2] *Security of Personal, Private and Sensitive Information (PPSI) in Mobile Computing Devices*, P2-12-10, December 14, 2012

[3] A binder that maintained sensitive student data was removed from a secretary's desk. The documents it contained were shredded because they could be accessed electronically.

social security numbers and student grades, medical or guardianship information, could be inadvertently exposed to, misused or altered by unauthorized users. Further, lack of information about the types and extent of data districts maintain – and where PPSI resides − can hamper efforts to properly notify affected parties in the event of a breach.

Data Backup

A backup is a copy of electronic information that is maintained for use if there is loss or damage to the original. Policies and procedures outlining the data backup process should include how often backups are to be performed, the process for verifying data has been properly backed up, information on storing the backup media in a secure location, and verifying the ability to restore the backup data.

While the Computer Services Department has written backup procedures, the descriptions are vague. Therefore, a new employee would not be able to follow them and obtain the desired result. Additionally, the current procedures do not name the individuals or titles of those who are responsible for restoring critical business functions in the event of a system malfunction, including any responsibilities of the third-party vendor that backs up the District's financial system. The Director of Computer Services also confirmed that the District has never tested its backup procedure to ensure the data could be restored. If the District's IT system was compromised, the District could lose essential information, including student records, which may not be recoverable. The District also could incur expenses for system restoration or for equipment repair or replacement.

Disaster Recovery Plan

A system of strong IT controls includes a disaster recovery plan that describes how an organization will deal with potential disasters. A disaster could be any sudden, unplanned catastrophic event such as a fire, flood, computer virus, vandalism or inadvertent employee action that compromises the integrity of the data and the IT systems. Contingency planning to prevent loss of computer equipment and data and the procedures for recovery in the event of an actual loss are crucial to an organization. The plan needs to address the roles of key individuals and include precautions to be taken to minimize the effects of a disaster so officials will be able to maintain or quickly resume day-to-day operations. In addition, disaster recovery planning involves an analysis of continuity needs and threats to business processes and may include a significant focus on disaster prevention. It is important for officials to distribute the plan to all responsible parties and to periodically test and update the plan to address changes in the District's IT security requirements.

The District's disaster recovery plan is inadequate because it is ambiguous and nondescript. While the plan states that the Director of

Computer Services and his or her staff must organize and maintain a computer emergency response team, the team has not been created. The plan does not provide details on how often the plan should be tested or updated. Further, the plan was last updated in 2008. In addition, the plan does not include details on the records and data that must be preserved during a disaster and does not designate alternate work locations. Consequently, in the event of a disaster or ransomware attack, District personnel have little guidance to help minimize or prevent the loss of equipment and data or to appropriately recover data. Without a comprehensive disaster recovery plan, the District could lose important data and suffer a serious interruption in District operations.

Recommendations

The Board should:

1. Adopt policies and procedures to address the classification of PPSI − including risk level definitions and requirements for updating classifications on an ongoing basis, as appropriate − and data backups.

2. Adopt and distribute a comprehensive disaster recovery plan to responsible parties that identifies how essential data will be preserved during a disaster and identifies alternate work locations. This plan should be periodically tested and updated.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

The District officials' response to this audit can be found on the following page.

Victor Central School District

953 High Street, Victor, New York 14564 (585) 924-3252 FAX: (585) 742-7090

Dawn A. Santiago-Marullo, Ed.D., Superintendent of Schools

www.victorschools.org

To Teach • To Learn • To Support • To Improve • To Achieve

June 22, 2016

Office of the State Comptroller
The Powers Building
16 West Main Street – Suite 522
Rochester, NY 14614

Office of the Comptroller:

Victor Central School District is in receipt of the Information Technology examination 2016M-117 for the period July 1, 2014 to March 4, 2016.

The report has two recommendations regarding Information Technology. The District will send the appropriate corrective action plan for the two items that were listed in the report after our School Board approves our responses.

On behalf of the Board of Education and the District's administration, we would like to thank the New York State Comptroller's field staff involved in the audit. They were courteous and professional throughout the process. The District is pleased with the extensive work of the auditors from your office and that the audit resulted in no findings of operational improprieties, fraud, waste, or abuse.

Sincerely,

Dawn A. Santiago-Marullo, Ed.D.
Superintendent of Schools

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

The objective of our audit was to review IT security for the period July 1, 2014 through March 4, 2016. To achieve our audit objective and obtain valid evidence, we performed the following procedures:

- We interviewed District officials to gain an understanding of IT operations.

- We reviewed District policies, Board minutes, financial reports and the CPA report and corrective action plan.

- To verify District bank transfers were appropriate, we traced bank transfers made in the month of January 2016 to other District bank accounts and followed up for additional documentation for transfers to non-District accounts. We selected January 2016 as the sample month because it was the most recent completed month with available bank statements.

- We reviewed the access rights to the financial software program for a randomly selected sample of five individuals.

- We reviewed information asset classification worksheets from December 5, 2013 through June 11, 2014 and interviewed a judgmentally selected sample of three departmental employees to verify the information on the worksheet.

We conducted this performance audit in accordance with 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.

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX D

OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

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

BUFFALO REGIONAL OFFICE
Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

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

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates Counties

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

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

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313