OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Rye Neck Union Free School District

Information Technology

Report of Examination

Period Covered:

July 1, 2014 – March 31, 2016

2016M-280

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

November 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 Rye Neck Union Free 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 Rye Neck Union Free School District (District) is located in the Town of Mamaroneck in Westchester County. The District is governed by a Board of Education (Board), which is composed of six elected members. The Board is responsible for the general management and control of the District's financial and educational affairs.

The Superintendent of Schools (Superintendent) 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 Assistant Superintendent for Business and Finance is responsible for the District's finances, maintaining the accounting records, preparing financial reports as well as assisting with the annual budgeting process. The District's budget for the 2015 - 2016 school year was approximately $39.6 million.

The District operates four schools with approximately 1,550 students and 230 employees. The District contracts out its information technology (IT) services.

Objective

The objective of our audit was to determine whether the District adequately safeguarded sensitive data stored on District computer systems. Our audit addressed the following related question:

- Did the Board and District officials provide adequate oversight of the District's IT systems?

Scope and Methodology

We examined the District's controls over IT for the period July 1, 2014 through March 31, 2016. 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's officials.

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 agreed with our recommendations and indicated that they plan on implementing corrective action.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the General Municipal Law, Section 2116-a (3)(c) of the 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

District officials are responsible for designing internal controls over the IT infrastructure used to store, retrieve and process data required to perform the District's mission of educating students. Internal controls must identify the data and clearly assign responsibility for protection of the data from unauthorized access. This includes classification of data by level of confidentiality, documenting the expected level of performance of IT vendors hired by the District and formal training of District employees with job responsibilities that require access to the data. In addition, the District must have a formal policy of when and how to notify persons when unauthorized access to their sensitive data stored by the District has occurred.

The Board and District officials need to improve controls over the District's IT assets. The Board did not establish adequate IT policies and procedures. We also found that the service level agreement (SLA) with the District's IT vendor is inadequate as it does not define all necessary aspects of the services provided to the District. As a result, the Board does not have adequate assurance that the District's IT assets are secure.

Policies and Procedures

Policies and procedures over IT are part of the internal control structure and provide criteria and guidance for District's computer-related operations. Effective protection of computing resources and data must include policies and procedures for classifying sensitive student and employee data, informing users about safe and acceptable use of District computers, providing District-wide IT security training and awareness and notifying effected individuals when there is a breach of data security. Computer users need to be aware of security risks and be properly trained in practices that reduce the internal and external threats to the network. The Board should periodically review and update these policies as necessary to reflect changes in technology or the District's computing environment. Additionally, record of IT security training provided and persons receiving the training should be maintained and reviewed to help identify when and what additional training should be provided.

The District has IT systems manuals containing Board-adopted IT policies and procedures. However, these manuals do not formally address certain critical areas of the IT systems to effectively protect the District's IT resources and data. Specifically, the District does not have adequate policies and procedures for personal, private and sensitive information (PPSI) data classification, acceptable use and cyber security training. In addition, there are no documented policies

or procedures for modifying user accounts and audit logs are not routinely generated and reviewed for unauthorized access or unusual activity.

Data Classification: PPSI – Our review of District's processing of PPSI and interviews of District officials and employees indicated the Board has not developed written policy and procedures for managing data the District collects, processes, transmits and stores. Board policy should define PPSI; explain the reasons for collecting PPSI; and describe specific procedures for the use of, access to, storage of and disposal of PPSI involved in the normal course of business.

We obtained the Internet browsing history from a sample of five computers and found PPSI in the uniform resource locators (URLs.)

Without formal policies and procedures, there is no assurance that data is effectively and adequately protected from unauthorized access. In addition, District officials and employees may not understand what constitutes sensitive information and how to adequately safeguard it. District officials may not be prepared to notify affected persons in a timely manner in case of a security breach.

Acceptable Use – Although the Board has established an acceptable use policy and procedures, we found instances where District officials did not ensure that they were completely followed. The District requires students and their legal guardians, as well as faculty, to sign off on the policy, which states that the District's network use is for "educational purposes and research consistent with the district's mission and goals." However, our review identified instances where employees used the District's network for activities (such as shopping, personal email, etc.) that did not comply with the acceptable use policy. Internet browsing increases the risk of exposing the District IT systems and data to malicious attacks.

Cyber Security Training – The Board has not developed adequate policy and procedures to ensure that District employees receive proper cyber security training to protect District IT assets. District officials informed us that they provided technical memos via email as well as elective training courses that require Superintendent approval. The lack of formal cyber security training increases the risk of District employees acting in a manner that could compromise District IT assets and security.

Web Filter

Due to the global nature of the Internet, school districts today find that it is a nearly indispensable resource for conducting legitimate business and educational activities. However, in recent years, even experienced users have been susceptible to significant threats from

cyber criminals who exploit the vulnerabilities of systems and software to gain unauthorized access to sensitive data. For example, computers can be infected by malicious software that, unknown to users, installs a keystroke logger that captures computer user identification and password information. Hackers can later use this information to access networks, databases and even bank accounts, resulting in high risk of loss.

Internet browsing increases the likelihood that users will be exposed to some form of malicious software that may compromise data confidentiality. The District should ensure there is an adequate web filtering process in place to limit vulnerabilities in District IT assets through web browsing and to ensure the District's network is only used for appropriate educational purposes.

The District's acceptable use policy provides employees and students with guidelines for IT asset use and security. Specifically, the policy prohibits the use of District computers for non-educational or illegal purposes. However, we found examples of viewable web filter categories that did not appear to be for educational purposes.

To evaluate web usage, we examined the web history for five District computers. We searched for website categories that appeared to be personal in nature rather than educational. District staff were able to access websites unrelated to District activities, such as personal online banking, an automobile dealership, insurance, personal email and social media. Although the acceptable use policy does not permit non-educational use, the web filter does not block categories that are frequently used for personal purposes.

When employees and students access websites for non-educational or inappropriate purposes through the District's network, productivity is reduced and there is an increased risk that the websites' contents could put District assets and users' information at risk of compromise through malicious software infections.

Service Level Agreement

In order to protect the District and to avoid potential misunderstandings, there should be a written agreement between the District and IT service providers that identifies the District's needs and expectations and specifies the level of service to be provided by the independent contractors/vendors. The components of the SLA should include identifying the parties to the contract, definitions of terminology, term/duration of agreement, scope/subject limitations, service level objectives and performance indicators, roles and responsibilities, nonperformance impact, security procedures, audit procedures, reporting requirements, review/update process, approvals, pricing, billing and terms of payment. Such contracts should establish measureable performance targets so that there is a mutual understanding of the nature and required level of service to be provided.

The District has a written SLA with its IT vendor. The SLA provides for the full-time, on-site service of one operations manager, one level II systems engineer and one level I systems engineer. The SLA defines the payment and scope of services. However, the SLA is not comprehensive because it does not have written terms defining the service level objectives and performance indicators, roles and responsibilities, nonperformance impact, security procedures, reporting requirements and review/update and approval processes.

The District's lack of a comprehensive SLA with the IT service provider could contribute to a lack of individual accountability for various aspects of the District's IT environment. As a result, the District's data and computer resources are at greater risk for unauthorized access, misuse or abuse.

Recommendations

The Board should:

1. Adopt IT policies and procedures related to IT security awareness training.

District officials should:

2. Inventory and classify by security level all PPSI maintained on District computer systems.

3. Ensure that employees receive formal IT security training on an ongoing basis that reflects current risks identified by the IT community.

4. Review and adjust as necessary the web content filtering setup to enforce staff and student compliance with the District's acceptable use policy.

5. Enforce the Board-adopted acceptable use policy.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

Rye Neck Schools
LEARN • ACHIEVE • LEAD

Peter J. Mustich, Ed.D.
Superintendent of Schools

November 2, 2016

Ms. Tenneh Blamah
Chief Examiner of Local Government & School Accountability
State of New York
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553

Dear Ms. Blamah,

The Board of Education and the district administration greatly appreciate the efforts of the auditing team from the Office of the State Comptroller. We offer the following brief comments to the draft report entitled Information Technology 2016M-280 for the period of July 1, 2014 to March 31, 2016 issued by the New York State Office of the State Comptroller for the Rye Neck Union Free School District.

The Comptroller's office conducted a comprehensive risk assessment of the District's finances involving various OSC staff and a total allocation of 130 work days to this audit. The risk assessment included a thorough evaluation of: Financial Condition and Oversight, Control Environment, Cash Receipts and Disbursements, Purchasing, Capital Assets and Consumable Inventories, Payroll and Personnel Services, Information Technology and Retirement Reporting to the New York State & Local Retirement System. The audit team did not find any fraud, waste or wrongdoing during the review which confirms the honesty and integrity of the District's staff. We are committed to following the highest standards of fiscal management. To that end, we have and will continue to support and implement improvements in our operations recommended by the Office of the State Comptroller.

The draft report made certain limited recommendations with respect to our IT policies and procedures. We take the Comptroller's recommendations seriously and respond as follows to them.

Recommendations

1. The Board should adopt IT policies and procedures related to IT security awareness training

We agree that security training is important and, consequently, we have added security awareness training to our list of required annual training for all employees.

310 Hornidge Road, Mamaroneck, NY 10543 | t: 914.777.5252 | f: 914.777.5251 | www.ryeneck.k12.ny.us

2. Inventory and classify by security level all PPSI maintained on District computer systems.

The district has undertaken and completed an inventory of PPSI that is maintained on district computer systems with a schedule developed to update annually.

3. Ensure that employees receive formal IT security training on an on-going basis that reflects current risks identified by the IT community.

We have added two modules to our required annual online training for our employees: Digital security and protection and classroom security and privacy awareness.

4. Review and adjust as necessary the web content filtering setup to enforce staff and students compliance with the District's acceptable use policy

The District agrees with the recommendation and will continue to work with our IT vendor to evaluate internet usage and block access to websites that do not comply with the acceptable use policy. We will work with our vendor to conform our filters to our policies.

5. Enforce the Board -adopted acceptable use policy

The district is in the process of reviewing and revising the acceptable use policy. The computer network coordinator shall monitor and examine all network activities, as appropriate, to ensure proper use of the system and enforcement of our use policy.

In conclusion, we would like to thank the Comptroller's Office and their field staff that performed our audit for their professionalism and hard work. We appreciate the recommendations and welcome the opportunity to improve our practices and procedures.

Sincerely,

Peter J. Mustich, Ed.D.
Superintendent of Schools

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

The objective of our audit was to determine if District officials ensured that PPSI on the District's computers was adequately safeguarded against unauthorized access and loss.

- We interviewed District officials and employees to determine procedures in place to protect PPSI stored on District computers.

- We interviewed employees of the District's IT vendor to determine what safeguards were in place to protect sensitive data.

- We reviewed written SLAs with the District's IT vendor to determine the scope of services, reporting requirements, performance indicators and security procedures to be provided to the District.

- We used the same judgmental sample of five computers and analyzed the web browsing history to identify questionable Internet use and pages that disclosed PPSI.

- We examined written Board policies to determine the amount and scope of policies officially adopted related to the protection of sensitive data.

- Used information system evaluation applications to determine if District information systems met industry standards regarding passwords, administrative access and configuration settings.

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