REPORT OF EXAMINATION | 2019M-193

Roosevelt Union Free School District

Information Technology

DECEMBER 2019

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

Contents

Report Highlights **1**

Information Technology **2**

How Can the District Help Prevent and Properly Respond to a Malicious Attack of Its IT System? 2

The Board Did Not Appoint a Chief Information Officer 3

The District Did Not Comply With Its IT Policies 3

The District Did Not Provide IT Security Awareness Training 4

The District Does Not Have a Disaster Recovery Plan 4

The Service Agreement With the IT Provider Is Inadequate 5

What Do We Recommend? 5

Appendix A – Response From District Officials **7**

Appendix B – OSC Comments on the District's Response **12**

Appendix C – Audit Methodology and Standards **13**

Appendix D – Resources and Services **14**

Report Highlights

Roosevelt Union Free School District

Audit Objective

Determine whether District officials established adequate controls to help prevent and properly respond to a malicious attack of the District's Information Technology (IT) system.

Key Findings

- The Board did not appoint a Chief Information Officer responsible for all IT matters.
- The Board did not adopt a disaster recovery plan.
- The District's IT Department did not provide employees and officials with IT security awareness training.

Key Recommendations

- Consider appointing a Chief Information Officer to be responsible for ensuring computerized data is secure, identifying and recommending technology solutions to the Board, ensuring IT users are appropriately trained and supervising IT Department staff.
- Adopt a disaster recovery plan.
- Ensure that computer users receive IT security awareness training and follow up training when District IT policies are updated.

District officials disagreed with certain findings in our report. Our comments on issues raised in the District's response are included in Appendix B.

Background

The Roosevelt Union Free School District (District) is located in the Town of Hempstead in Nassau County.

The five-member Board of Education (Board) is responsible for managing financial and educational affairs. The School Superintendent is responsible for day-to-day management and administration under the Board's direction.

The three-member technology team, comprised of the lead IT Specialist, Coordinator of Instructional Technology, and Assistant Superintendent for Elementary Education, is collectively responsible for the District's IT matters.

Quick Facts	
Students	3,697
Employees	520
2019-20 General Fund Appropriations	$104 million
2019-20 Information Technology Appropriations	$1.1 million

Audit Period

July 1, 2018 – June 30, 2019

Information Technology

The District relies on its IT system for Internet access, email, and maintaining and accessing financial and personal records. Therefore, the IT systems and data are valuable District resources. If IT systems are compromised, the results could range from inconvenient to severe and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of an IT system, a lack of effective controls significantly increases the risk that data, hardware and software may be lost or damaged by a malicious attack of the District's IT system.

How Can the District Help Prevent and Properly Respond to a Malicious Attack of Its IT System?

The Board should appoint a Chief Information Officer (CIO) in charge of and responsible for all IT matters. The CIO should communicate technology needs to the Board and be responsible for training users and ensuring all computerized data is secured. The CIO's responsibilities should include supervising IT Department employees, identifying and eliminating security risks, and identifying and recommending new technology solutions to the Board.

The District's IT policy requires all staff to provide a written agreement that their use of computers will conform to the District's acceptable use policy. In addition, all employees and authorized users are required to annually acknowledge their agreement to follow the District's acceptable computer use policy. The District's Internet safety policy requires District officials to disseminate the acceptable use policy to parents and students so they are aware of the District's expectations and students' obligations when accessing the Internet.

The District should provide, and require employees and officials to attend, periodic IT security awareness training that explains the proper rules of behavior for using IT systems and data. Security awareness training communicates IT security expectations to employees, helps them recognize security concerns and react appropriately, and helps them understand their individual responsibilities.

A disaster recovery plan (DRP) should be adopted to anticipate and plan for an IT disruption involving the corruption or loss of data. The plan should be tested to ensure that employees and officials understand their roles and responsibilities in a disaster situation. A DRP, sometimes referred to as a business continuity plan or business process contingency plan, describes the plans, policies, procedures and technical measures for the recovery of IT operations after a destructive event. Such events could include a natural disaster (such as a flood), human error, hardware failure or malfunctioning software caused by malware or a computer virus, such as ransomware. Periodic backup of critical systems and data is essential to recovery of operations. Backup media should be periodically tested to ensure it is in a useable format.

The District should have a written service agreement with its IT service provider that identifies the term of the agreement, scope, objectives, roles and responsibilities, and pricing. A vague agreement can lead to the District's needs and expectations not being met.

The Board Did Not Appoint a Chief Information Officer

The Board did not appoint a CIO in charge of and responsible for all IT matters. Instead, the District's IT Department is comprised of four IT Specialists provided by the Nassau Board of Cooperative Education Services (BOCES) and a Secretary that is a District employee. The lead IT Specialist (IT Specialist) reports to the District's Coordinator of Instructional Technology (Coordinator), and the Coordinator reports to the Assistant Superintendent for Elementary Education (Assistant Superintendent).

The District's technology team, comprising the lead IT Specialist, the Coordinator and the Assistant Superintendent, meets weekly to discuss IT matters. The District relies on the IT Specialist to recommend IT acquisitions or other IT system security changes. The recommendations must be approved by the Coordinator. District officials told us that because the IT Specialist and Coordinator generally disagree, the Assistant Superintendent is left to decide whether to implement the IT Specialist's recommendations. However, the Assistant Superintendent does not have an IT background.

Without a CIO, the Board did not assign responsibility to any one individual to establish policies and procedures to help prevent and properly respond to a malicious attack of its IT system. As a result, it is unclear which District official is responsible for all IT matters, including communicating technology needs to the Board, training users and ensuring all computerized data is secured.

The District Did Not Comply With Its IT Policies

The District's IT Coordinator told us that the District does not maintain a written agreement on file for each staff member indicating that the staff member's computer use will conform to the District's acceptable use policy. Also, employees and authorized users do not annually acknowledge their agreement to follow the District's acceptable use policy, as required by the IT policy. Lastly, we were told that officials did not disseminate the acceptable use policy to parents and students, as required by the District's Internet safety policy.

District officials failed to comply with their own IT policies. As a result, users may not be aware of the District's requirements, expectations and the users' obligations when accessing the Internet and email. This places the District's IT system at greater risk for malicious attacks because users are likely to go to websites with greater risk of infection.

The District Did Not Provide IT Security Awareness Training

The District did not provide employees and officials with IT security awareness training. Instead, the District's IT Coordinator occasionally emails staff to inform them of cyber security threats. For example, in February 2019 the Coordinator emailed District staff to explain phishing[1] and malicious emails and provide tips to protect users and the District from these attacks. However, these informal procedures are not reinforced with periodic IT security awareness training to ensure that all computer users are aware of security concerns, their individual responsibilities and how to react appropriately to phishing and ransomware[2] attacks.

The District does not have a formal IT security awareness training plan that identifies individuals required to complete the training and the frequency at which the training will be provided. As a result, computer resources and data with which users have been entrusted are at greater risk for malicious attacks. This risk is compounded because, without procedures to limit the sites that users go to, there is greater risk of being subject to attack. Without training, users are less likely to know how to respond when phishing or other attacks occur.

The District Does Not Have a Disaster Recovery Plan

The Board and District officials have not developed and adopted a written DRP. Officials provided us with a draft DRP that was created in November 2018 by the District's Educational Technology Coordinator (Coordinator) using a BOCES DRP template. However, the Coordinator informed us that he has not worked on the draft DRP since that time and is unaware of the draft's status.

In addition, the District does not have a regular method in place for testing backups. The IT Department restores backups when users request the restoration of certain files or information.

Without a Board-adopted DRP, District officials have no guidance on how to help minimize or prevent the loss of data or how to appropriately recover data in the event of a disaster or a phishing or ransomware attack. The District could lose important financial and other data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees or process student grades and State aid claims. With the current, and growing, prevalence of ransomware and other malware attacks, the need for a DRP is of utmost importance. Given the lack of acceptable use policies or security awareness training, it is even more important for the District.

1 Phishing is sending deceptive email messages in an attempt to gather personal information or infect computer systems with malicious software.

2 Ransomware is a type of malicious software that prevents users from accessing their computer systems or electronic data until a ransom payment is made.

The Service Agreement With the IT Provider Is Inadequate

The District does not have a written agreement with BOCES that clearly states the IT services to be provided. Rather, the Assistant Superintendent for Business provided us with a contract for cooperative education services which contained standard boilerplate language and pricing of the IT services that would be provided by BOCES during the 2018-19 school year. For example, the District paid $143,586 for outsourced network support. However, District officials could not explain what specific services are covered under outsourced network support.

The District relied on a vague contract for cooperative education services instead of entering into a detailed written service agreement with BOCES. As a result, there is no clear understanding of BOCES' responsibilities and District officials are not sure what IT functions need to be performed in-house and which services are outsourced. This could result in the District paying for IT services it does not need or services that it expects to, but does not, receive. For example, the District's IT services agreement with BOCES includes intrusion detection system (IDS)[3] services. However, as a result of our audit inquiries, BOCES staff became aware that the IDS software was not properly configured to alert them of unusual or unauthorized events. As a result, the District paid for IDS services that it did not receive and, therefore, did not benefit from the additional security a properly configured IDS provides to its IT system.

What Do We Recommend?

The Board should:

1. Review, and update as needed, the IT policies and then require compliance with these policies.
2. Require periodic security awareness training for all authorized computer users.
3. Consider appointing a Chief Information Officer to be responsible for all IT matters, including, but not limited to, ensuring computerized data is secure, identifying and recommending technology solutions to the Board, ensuring IT users are appropriately trained and aware of District IT use policies, and supervising IT Department staff.
4. Adopt a comprehensive written disaster recovery plan.

3 An IDS can identify unauthorized, unusual and sensitive access activity and alert the Network Administrator of such events. Events identified by the IDS can then be reviewed and any apparent or suspected violations investigated.

5. Ensure that the District enters into a written service agreement with its IT service provider which identifies the term of agreement, scope, objectives, roles and responsibilities, and pricing.

6. Request reimbursement from BOCES for any IDS services the District paid for but did not receive.

The District's IT Department, under the direction of a CIO or the District's Coordinator, should:

7. Properly configure its IDS to alert the on-site IT Specialist of unusual or unauthorized events.

8. Investigate all events identified by the IDS and take corrective action, as needed.

9. Ensure that computer users receive IT security awareness training and provide follow-up training when District IT policies are updated.

10. Periodically test backups.

Appendix A: Response From District Officials

November 26, 2019

Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788

Dear Mr. McCracken:

The Roosevelt Union Free School District has reviewed the draft Report of Examination of Information Technology conducted by the Office of the State Comptroller (OSC) for the period of July 1, 2018 – June 30, 2019. This document serves as the District's response and Corrective Action Plan to the draft report.

The Board of Education and School District Administration wishes to thank your office for conducting the detailed examination of internal controls over Information Technology. The District is pleased that the report indicates that the Board of Education, School District Administration and business office staff worked cooperatively with your audit team. The District appreciates the input from the Office of the State Comptroller and will follow the recommendations offered in the report as we continue our efforts to ensure that best practices are implemented in all aspects of School District procedures and operations.

If any additional information is needed, please do not hesitate to contact my office.

Sincerely,

Eva J. Demyen
Acting Superintendent of Schools

Administrative Offices 240 Denton Place, Roosevelt, NY 11575, Tel: 516.345.7021 Fax: 516.345.7320

Unit Name: ROOSEVELT UNION FREE SCHOOL DISTRICT
Audit Report Title: Information Technology – Report of Examination 2019M-193
Audit Report: July 1, 2018 – June 30, 2019

Recommendation #1
The Board should review, and update as needed, the IT policies and then require compliance with these policies.

Implementation Plan of Action(s):
District staff and stakeholders have always been required to be compliant with Board IT policies. The Board has reviewed and will update IT policies and continue to require compliance with the updated policies. A file will be maintained of employees' acknowledgement of receipt of said policies, and employees will be held accountable for policy infractions.

Implementation Date:
December 4, 2019

Person Responsible for Implementation:
Board of Education, Superintendent of Schools, Chief Information Officer

Recommendation #2
The Board should require periodic security awareness training for all authorized computer users.

Implementation Plan of Action(s):
The District has been providing security awareness training for authorized computer users and will ensure that all authorized computer users are trained by the end of the year. Training has been scheduled for those authorized computer users. A file is being maintained in Human Resources of authorized users' acknowledgment of the completion of these trainings.

See Note 1 Page 12

Implementation Date:
December 31, 2019

Person Responsible for Implementation:
Board of Education, Superintendent of Schools, Chief Information Officer

Recommendation #3
The Board should consider appointing a Chief Information Officer to be responsible for all IT matters, including, but not limited to, ensuring computerized data is secure, identifying and recommending technology solutions to the Board, ensuring IT users are appropriately trained and supervising IT Department staff.

Implementation Plan of Action(s):
The Board has appointed a Chief Information Officer whose responsibility it is to ensure that computerized data is secure, identify and recommend technology solutions to the Board, ensure IT users are appropriately trained, and supervise IT Department staff.

Unit Name: ROOSEVELT UNION FREE SCHOOL DISTRICT
Audit Report Title: Information Technology – Report of Examination 2019M-193
Audit Report: July 1, 2018 – June 30, 2019

Implementation Date:
Complete

Person Responsible for Implementation:
Board of Education, Superintendent of Schools, Chief Information Officer

Recommendation #4
The Board should adopt a comprehensive written disaster recovery plan.

Implementation Plan of Action(s):
The Board had a first reading of a comprehensive disaster recovery plan and is set to adopt the plan at its December 4, 2019 Board of Education meeting.

Implementation Date:
December 4, 2019

Person Responsible for Implementation:
Board of Education, Superintendent of Schools, Chief Information Officer

Recommendation #5
The Board should ensure that the District enters into a written service agreement with its IT service provider which identifies the term of agreement, scope, objectives, roles and responsibilities, and pricing.

Implementation Plan of Action(s):
BOCES has agreed to provide the District with "written service agreements and other elements as noted," in addition to the standard AS-7 contract and Letter of Intent that it provides its component districts.

Implementation Date:
December 4, 2019

Person Responsible for Implementation:
Board of Education, Superintendent of Schools, Chief Information Officer, Assistant Superintendent for Business

Unit Name: ROOSEVELT UNION FREE SCHOOL DISTRICT
Audit Report Title: Information Technology – Report of Examination 2019M-193
Audit Report: July 1, 2018 – June 30, 2019

Recommendation #6
The Board should request reimbursement form BOCES for the IDS services the District paid for but did not receive.

Implementation Plan of Action(s):
BOCES had two conference calls with the auditors and asserts that "the district has appropriately configured 'Intrusion Prevention Services" configured on its firewall that have been present since the device was installed. BOCEs maintains that "this is quite simply a misunderstanding related to semantics as the term IDS ("Intrusion Detection Services) has been largely replaced on many security appliances with "IPS". The policies on the [redacted] appliance are configured to automatically block threats and vulnerabilities." For further clarification the link below is provided:

See Note 2 Page 12

[redacted]

Implementation Date:
Complete

Person Responsible for Implementation:
Board of Education, Superintendent of Schools, Chief Information Officer

Recommendation #7
The District's IT Department, under the direction of a CIO or the District's Coordinator, should properly configure its IDS to alert the on-site IT Specialist of unusual or unauthorized events.

Implementation Plan of Action(s):
The District's IPS has been configured to forward events daily to the lead tech in the District who investigates the alerts. The Chief Information Officer is apprised of all alerts and works with the BOCES IT Specialist to take corrective action.

See Note 2 Page 12

Implementation Date:
Complete

Person Responsible for Implementation:
Chief Information Officer

Recommendation #8
The District's IT Department, under the direction of a CIO or the District's Coordinator, should investigate all events identified by the IDS and take corrective action, as needed.

Implementation Plan of Action(s):
The District's IPS has been configured to forward events daily to the lead tech in the District who investigates the alerts. The Chief Information Officer is apprised of all alerts and works with the BOCES IT Specialist to take corrective action on all events identified.

See Note 2 Page 12

Unit Name: ROOSEVELT UNION FREE SCHOOL DISTRICT
Audit Report Title: Information Technology – Report of Examination 2019M-193
Audit Report: July 1, 2018 – June 30, 2019

Implementation Date:
Complete

Person Responsible for Implementation:
Chief Information Officer

Recommendation #9
The District's IT Department, under the direction of a CIO or the District's Coordinator, should ensure that computer users receive IT security awareness training and provide follow up training when District IT policies are updated.

Implementation Plan of Action(s):
The District has been providing security awareness training for authorized computer users and will ensure that all authorized computer users are trained by the end of the year, once IT policies have bee updated.

See Note 1 Page 12

Implementation Date:
December 31, 2019

Person Responsible for Implementation:
Chief Information Officer

Recommendation #10
The District's IT Department, under the direction of a CIO or the District's Coordinator, should periodically test backups.

Implementation Plan of Action(s):
The District replicates all data off site nightly through SAN replication; this is checked daily. File level backups provided through [redacted] are also checked daily. BOCES technicians will now schedule a file level restore "test" to be done and verified weekly.

Implementation Date:
Ongoing

Person Responsible for Implementation:
Chief Information Officer

Appendix B: OSC Comments on the District's Response

Note 1

The District did not provide employees and officials with IT security awareness training during our audit period. Instead, the District's IT Coordinator occasionally emailed staff to inform them of cyber security threats. These informal procedures were not reinforced with periodic IT security awareness training to ensure that all computer users are aware of security concerns, their individual responsibilities and how to react appropriately to phishing and ransomware attacks.

Note 2

During audit fieldwork, we discussed the importance of a properly configured system with District officials. Regardless of whether the District uses an IDS or an IPS, our intention was to emphasize with District officials that the system was not functioning properly. In a November 13, 2019 conference call between BOCES and OSC auditors where District officials were present, a BOCES official confirmed that the District's system was not properly configured and the on-site IT Specialist at the District was not receiving alerts of unusual or unauthorized events as he should have been. As a result, the District paid for services that it did not receive and, therefore, did not benefit from the additional security a properly configured system provides.

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 reviewed adopted IT policies and interviewed District officials and the District's IT service provider to gain an understanding of the District's IT operations.
- We reviewed the District's 2018-19 BOCES contract for cooperative educational services to determine whether the District had a written service agreement with its IT service provider.

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.

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.

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 General Municipal Law, Section 2116-1(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. We encourage the Board 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/pubs/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/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

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief Examiner

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533

Tel (631) 952-6534 • Fax (631) 952-6091 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties

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