REPORT OF EXAMINATION | 2018M-22

Oyster Bay-East Norwich Central School District

Information Technology

JUNE 2018

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

Contents

Report Highlights **1**

Information Technology **2**

How Should District Officials Protect the PPSI on the Financial Server? 2

District Officials Did Not Provide Cybersecurity Awareness Training 2

District Officials Did Not Disable or Remove Unnecessary User Accounts 3

What Do We Recommend? 3

Appendix A – Response From District Officials **4**

Appendix B – Audit Methodology and Standards **5**

Appendix C – Resources and Services **6**

Report Highlights

Oyster Bay-East Norwich Central School District

Audit Objective

Determine whether District officials ensured that the personal, private and sensitive information (PPSI)[1] maintained on the District's financial server was adequately protected from unauthorized access, use and loss.

Key Findings

District officials did not:

- Provide cybersecurity awareness training to all employees.
- Disable or remove unnecessary user accounts in a timely manner.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Provide employees with periodic cybersecurity awareness training.
- Ensure user accounts are disabled or deleted as soon as no longer needed.
- Address the IT recommendations communicated confidentially.

District officials generally agreed with our recommendations and have initiated, or indicated they planned to initiate, corrective action.

Background

The Oyster Bay-East Norwich Central School District (District) serves the Town of Oyster Bay in Nassau County. The Board of Education (Board), which comprises seven elected members, is responsible for the general management and control of the District's educational and financial affairs. The Superintendent of Schools, the District's chief executive officer, along with the Assistant Superintendent for Finance and Operations, are responsible for the District's day-to-day management under the Board's direction.

Quick Facts	
Schools	3
Students	1,573
Employees	458

Audit Period

July 1, 2015 – October 23, 2017

1 PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, customers (residents), third parties or New York residents in general.

Information Technology

District officials collect and maintain a variety of PPSI including employee names, addresses, birth dates and Social Security numbers on the District's financial server. Access to PPSI on the financial server is managed by using network user accounts. District officials rely on the computers, software programs and other information technology (IT) to safeguard and manage PPSI. These IT assets must be properly safeguarded to protect PPSI against unauthorized access, misuse and loss. This is especially important given the increase in cybersecurity attacks including viruses, ransomware and other types of malicious software (malware).[2]

How Should District Officials Protect the PPSI on the Financial Server?

The IT security community often identifies people as the weakest link in the chain for securing data and systems, which includes PPSI on the District's financial server. Good IT controls include providing employees with cybersecurity awareness training at least annually. Such training should, at a minimum, address current risks identified by the IT community such as computer use, phishing and social media.

To minimize the risk of unauthorized access, District officials should regularly review the enabled network user accounts to ensure that they are still needed. Access should be terminated when students graduate and employees leave the District or no longer need access to perform their job duties. Unnecessary accounts should be promptly disabled and unnecessary user rights should be terminated. Such controls will help limit the risk that PPSI will be exposed to unauthorized access, misuse and loss.

District Officials Did Not Provide Cybersecurity Awareness Training

District officials did not ensure that employees, at least annually, receive cybersecurity awareness training. According to officials, they provided their employees with verbal and written reminders and specific directives regarding data security and computerized information. An official told us that the District's attorneys recently provided the faculty with information on data security and privacy and answered faculty questions on this matter. However, the Business Office employees and other clerical staff, who have access to the financial system and PPSI, did not receive that information. Officials provided no other documentation to support efforts to provide cybersecurity awareness training. As a result, users may not be prepared to recognize and appropriately handle malicious email messages, which increases the risk of a ransomware or other

2 Malware refers to programs specifically designed to harm computers and data. Ransomware is a type of malware that restricts access to a computer it infects or the data that computer contains and then demands that a ransom be paid to regain access.

type of malware infection on the District's computers. Therefore, the District's IT assets and PPSI are more vulnerable to unauthorized access, misuse and loss.

District Officials Did Not Disable or Remove Unnecessary User Accounts

We examined 5,551 enabled network user accounts (2,764 on one system and 2,787 on another system) to determine whether they are in accordance with industry best practices. We found 3,118 user accounts (56 percent) that had not been used in over six months. After we brought this to their attention, District officials said they disabled or deleted all of the 2,764 unnecessary user accounts from the one system. For the other system containing 2,787 user accounts, during our audit, District officials said they disabled or deleted 20 accounts and that most of the unused accounts belong to current and former students. Officials said it was a District practice to maintain each graduated student's user account for two years from the student's graduation. We also found 379 active generic/shared user accounts. After this was brought to their attention, District officials said they disabled/deleted 202 of the generic/shared accounts.

User accounts on a network are potential entry points for attackers as they could be used to inappropriately access and view PPSI in the financial system. Further, unnecessary user accounts create additional work when managing access to the District's network. To decrease the risk of unauthorized access, it is imperative that District officials disable or remove unnecessary accounts as soon as they determine there is no longer a need for them. Further, because generic/shared user accounts are not assigned to a single user, District officials may have difficulty managing these accounts and linking any suspicious activity to a specific user.

What Do We Recommend?

District officials should ensure that:

1. Employees periodically receive cybersecurity awareness training.
2. Unnecessary accounts are disabled or removed in a timely manner.

Appendix A: Response From District Officials

Oyster Bay - East Norwich Central School District

1 McCouns Lane

Oyster Bay, New York 11771-3105

516-624-6500 • Fax 516-624-6520

www.obenschools.org

May 4, 2018

The Board of Education and the Administration of the Oyster Bay- East Norwich School District appreciate the efforts of your office as well as the time and effort devoted to the analysis of Information Technology for the period beginning on July 1, 2015 and ending on October 23, 2017. The School District appreciates the comments and recommendations by the Office of the State Comptroller. The audit recommendations will be of assistance in the District's continuing efforts to implement best practices in all aspects of our operations.

The School District's response to the two audit findings are included here:

1. Employees periodically receive cybersecurity awareness training.

We have received information and are actively pursuing training for all of our employees regarding cyber security training. Business Office training for this topic has already been scheduled. We understand that this training in this key area of operations is important. The training will include the utilization of safe and secure business habits, software concerns, using strong passwords, online security concerns and being aware and mindful about the possibility of security threats.

2. Unnecessary accounts are disabled or removed in a timely manner:

Unnecessary user accounts have been deactivated. There is a comprehensive system in place for adding and deleting users.

Thank you for your time and attention. We look forward to working with the Office of the State Comptroller in efforts to safeguard assets and strengthen controls in the ever- changing area of technology. Please do not hesitate to contact me if you have any additional questions.

Sincerely,

Dr. Laura Seinfeld

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We interviewed District officials and reviewed certain District's records to determine if employees received cybersecurity awareness training.
- We used audit scripts to analyze and assess network user accounts and the security settings applied to those accounts.

Our audit also examined the adequacy of certain IT 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 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 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 C: 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/lgli/pdf/cybersecurityguide.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

APPLIED TECHNOLOGY UNIT – Randy Partridge, Chief Examiner

110 State Street • Albany, New York 12236

Tel: (518) 486-9881

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