REPORT OF EXAMINATION | 2017M-246

Cairo-Durham Central School District

Information Technology

FEBRUARY 2018

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

Contents

Report Highlights

Cairo-Durham Central School District

Audit Objective

Determine whether District officials properly safeguarded information technology (IT) assets.

Key Findings

- IT-related policies were not adequate.
- Users accessed websites unrelated to business activities, and web filters were not adequate.

In addition, sensitive IT control weaknesses were communicated confidentially to District officials.

Key Recommendations

- Update the District's IT policies.
- Require District employees to attend cybersecurity and awareness training.
- Monitor Internet usage and configure the web filtering software to block access to sites that violate the acceptable use policy.
- Address the IT recommendations communicated confidentially.

District officials generally agreed with our findings and indicated that they have taken, or plan to take, corrective action. Appendix B contains our comment regarding an issue raised in the District's response letter.

Background

The Cairo-Durham Central School District (District) serves the Towns of Cairo, Durham, Athens, Catskill, Coxsackie and Greenville in Greene County, Conesville in Schoharie County, and Rensselaerville in Albany County.

The District is governed by a Board of Education (Board) composed of nine elected members. The Board is responsible for developing policies, rules and regulations for managing the District.

The School Network Administrator is responsible for managing the District's IT access. The District uses network and web resources to support business operations, including financial records, student records, online banking, and communication.

Quick Facts	
Employees	269
Enrollment	1,200
2016-17 Appropriations	$28,966,155
2016-17 IT Budget	$839,022

Audit Period

July 1, 2015 – June 27, 2017

We extended our scope to the end of fieldwork (October 6, 2017) to complete computer testing.

Information Technology

How Can School Officials Safeguard IT Assets?

Policies over IT should provide criteria and guidance for computer-related operations. Effective protection includes an acceptable use policy for the appropriate and safe use of district computers, policies and procedures for classifying sensitive student and employee data, policies outlining appropriate wireless connection to the network, District-wide IT security and awareness training, and a breach notification process to inform affected individuals if there is a data security breach. The board should periodically review and update these policies to reflect changes in technology or the computing environment. 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.

School districts are susceptible to threats from cybercriminals who exploit the vulnerabilities of IT systems to gain unauthorized access to sensitive data. For example, computers can be infected by malware that installs a keystroke logger to capture identification and password information. Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality. District officials can reduce the risks to sensitive data and IT assets by monitoring Internet usage, and by using web filtering software to block access to unacceptable websites and limit access to sites that comply with the acceptable use policy.

IT Policies Are Not Adequate

The District's IT policies and procedures were not adequate. Although the District had computer/Internet use policies, they have not been revised for changes in technology since December 2006. In addition, the Board has not adopted policies and procedures for personal, private and sensitive information (PPSI) data classification, wireless security, managing mobile computing and storage devices, and cybersecurity training. The District also does not have written procedures for granting, changing and terminating access rights to the networked computer system and to specific software applications.

Without IT policies, users may not know how to appropriately use the District's network, devices and PPSI. In addition, without procedures for granting, changing and terminating access rights, users may have more access than necessary. As a result, the District may be exposed to malicious attacks that could compromise systems and data by putting computers at risk for viruses or malicious software (malware).[1]

1 Malware infiltrates a computer system by circumventing network defenses, avoiding detection and restricting efforts to disable it.

Cybersecurity Training Is Not Provided to District Employees and Staff

To protect the confidentiality, integrity and availability of District data and computer systems, District officials must ensure that employees who use and manage IT understand the District's security policies and procedures and know their related roles and responsibilities. In conjunction with policies and procedures, appropriate training should address:

- Emerging trends in information theft and other social engineering reminders;
- Limiting the type of PPSI collected, accessed or displayed to essential information for the function performed;
- Guarding against malicious software;
- The importance of virus protection;
- The dangers of downloading files and programs from the Internet;
- Key controls for passwords and wireless networking security; and
- How to respond to a virus threat or an information security breach.

The District does not provide, or require employees to attend, any formal cybersecurity awareness training. As a result, there is an increased risk that District employees will compromise District IT assets and security, placing the District at greater risk.

Internet Usage Is Inappropriate and Web Filters Are Inadequate

We selected and reviewed a judgmental sample of 11[2] District computers. District staff were able to access websites unrelated to District activities, such as games, hobby sites, job searching, social media, shopping and travel. This occurred because District officials did not sufficiently configure the web filtering software to block access to these sites. Further, we reviewed the web filter configurations to determine whether they adequately applied the District's acceptable use policy to the settings.

In addition to the websites that employees actually accessed on the sampled computers, the web filter allows potential access to sites in categories including terrorism, adult entertainers and gambling. Inappropriate use of District computers could potentially expose students to inappropriate content, or the District to virus attacks that compromise systems and data, including key financial and confidential information.

2 We selected all six of the Business Office computers that are used to conduct online banking activities and five other computers that have access to certain sensitive data. See Appendix C for additional detail.

What Do We Recommend?

The Board should:

1. Update the District's IT policies to include the current technology environment.

2. Provide periodic cybersecurity training to District employees.

District officials should:

3. Monitor Internet usage and configure the web filtering software to block access to sites that violate the acceptable use policy.

Appendix A: Response From District Officials

Cairo-Durham Central School District **Office of the Superintendent**
P. O. Box 780, Cairo, New York 12413-0780 Anthony J. Taibi
Phone: (518) 622-8534 Superintendent of Schools
Fax: (518) 622-9566 www.cairodurham.org

Office of the State Comptroller
Newburgh Regional Office
33 Airport Center Drive, Suite 103
New Windsor, New York 12553

Dear Chief Examiner Blamah,

The purpose of this letter is to acknowledge receipt of the preliminary draft findings report, titled "Information Technology, Report of Examination" conducted by the Office of the State Comptroller.

The Board of Education and District Administration are appreciative of the efforts of the auditing team as well as their exhibited professionalism. Through the auditing process, we were able to examine current practices and make necessary adjustments. In several key areas identified in the preliminary findings, the district has already taken steps to correct the identified issues. Overall, the district is in agreement with the audit findings, however, the district would like to address a few minor areas prior to the issuance of the final report.

Cybersecurity - In response to the statement on page 5, "Cybersecurity Training is not provided to district employees and staff." While the adopted Board of Education policies cover this area, and all staff are expected to have knowledge of and adhere to these policies, the district fully agrees that explicit training for all staff is necessary in order to ensure that the confidentiality and integrity of district data is maintained.

Internet Usage - In response to the statement that "District staff were able to access websites unrelated to District activities, such as games, hobby sites, job searching, social media, shopping and travel." The Board of Education and District Administration fully agree that activity unrelated to curricular or job related tasks, specifically for personal business, is not appropriate and should not occur. On balance, the district would like to point out that filtering settings that are too restrictive could limit or hinder the ability of students and teachers to access information relevant to district curriculum.

See Note 1 Page 6

District Information Technology Policies - The district fully agrees with the assessment that several important policies are out of date and need to be updated. The Board of Education and District Administration are already actively engaged in the update of these policies in order to ensure that these are current.

Once finalized the district will prepare and send the appropriate, comprehensive Corrective Action Plan for all items identified in the report.

On behalf of the Cairo-Durham Central School District and the Board of Education, we would like to thank the Office of the State Comptroller staff for their professionalism as well as the comprehensive report that has been submitted to the district

Sincerely,

Anthony J. Taibi
Superintendent of Schools

Appendix B: OSC Comment on the District's Response

Note 1

The websites allowed by the District could expose students to inappropriate content and could also expose the District's network to virus attacks that compromise systems and data.

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, we performed the following audit procedures:

- We reviewed the District's policy and procedure manuals to identify IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.
- We interviewed officials and personnel to gain an understanding of internal controls over IT.
- We selected and examined six computers by running audit software and examined specific activities on those computers, such as software inventory, to identify virus protection software and definition updates.
- We selected 11 computers and reviewed web history reports for accessed websites that violated the District's acceptable use policy or could put the District's network at risk. We selected six computers (those assigned to the Treasurer, Deputy Treasurer, Extra Classroom Activities Treasurer and Assistant Superintendent for Business)[3] because the officials' duties and privileges involved using and transmitting important electronic data. We selected five other computers used by various employees because they had permission to use the individualized education plan application, which contained PPSI. We selected the five computers by using a spreadsheet random number generator to select from the 88 employees with permission to the application.

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.

3 The Treasurer and the Assistant Superintendent for Business were each assigned a desktop and laptop computer.

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 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/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.state.ny.us

www.osc.state.ny.us/localgov/index.htm

Local Government and School Accountability Help Line: (866) 321-8503

NEWBURGH REGIONAL OFFICE – Tenneh Blamah, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.state.ny.us

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

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