REPORT OF EXAMINATION | 2019M-46

Cazenovia Central School District

Information Technology

JULY 2019

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

Contents

Report Highlights

Cazenovia Central School District

Audit Objective

Determine whether District officials ensured that the personal, private and sensitive information (PPSI) on District servers and in the financial system was adequately protected from unauthorized access, use and loss.

Key Findings

District officials did not:

- Provide cybersecurity awareness training to employees.
- Disable and/or remove unnecessary user accounts on the network.
- Properly manage PPSI data.

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

Key Recommendations

- Provide employees with periodic cybersecurity awareness training.
- Adopt policies and procedures for adding, deleting and modifying user access rights.
- Inventory, classify and develop controls over PPSI maintained and collected by the District.

District officials agreed with our recommendations and indicated they would initiate corrective action.

Background

Cazenovia Central School District (District) serves the Towns of Cazenovia, Fenner, Georgetown, Lincoln, Nelson and Sullivan in Madison County and the Town of Pompey in Onondaga County. The Board of Education (Board), which is composed of seven elected members, is responsible for the general management and control of the District's educational and financial affairs. The Superintendent of Schools (Superintendent) is the chief executive officer and is responsible, along with other administrative staff, for the day-to-day management under the Board's direction.

The District's IT Department consists of a Technology Coordinator, who works remotely from South Carolina, two computer services technicians, a computer support technician and a computer support specialist.

Quick Facts	
Number of Schools	3
Number of Students	1,432
Number of Employees	334
2018-19 Budget Appropriations	$29.7 million
Employee and Student User Accounts	1,840

Audit Period

July 1, 2017 – August 31, 2018

Information Technology

The District relies on its information technology (IT) assets for Internet access, email and for maintaining financial, personnel and student records and data that may involve personal, private or sensitive information (PPSI).[1] Therefore, the IT systems and data are valuable resources that need to be protected from unauthorized and inappropriate use. If the IT assets are compromised, the results could range from inconvenient to significant damage and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of assets and data, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

How Should District Officials Protect PPSI?

A well-informed work force is a strong link in the chain to secure electronic data and computer systems. In order to protect the confidentiality, integrity and availability of district data and systems, the board and district officials should develop and communicate written IT security policies and procedures and ensure that the people who use and manage IT understand their roles and responsibilities related to IT security.

Accordingly, the board should adopt an acceptable use policy that defines the procedures for computer, Internet and email use and ensure that IT security awareness training is periodically provided to staff who use IT resources. In addition, officials should develop and communicate written procedures for storing, classifying, accessing and disposing of PPSI. The board should also adopt a breach notification policy that details how officials would notify individuals whose private information was, or is reasonably believed to have been, acquired without valid authorization.

To minimize the risk of unauthorized access, officials should have established policies and procedures on adding, removing and modifying user access rights to the district's network and financial application and should periodically review and compare assigned user access rights to job duties to ensure they are current and appropriate. Unnecessary accounts should be promptly disabled and unnecessary user rights should be terminated. Furthermore, the district should limit the number of generic or shared user accounts because these accounts are not assigned to a single user and can be difficult in managing and linking suspicious activity to a specific user.

Finally, officials should develop a disaster recovery plan to prevent the loss of computerized data and assets and to ensure that operations can resume in

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 (students), third parties or citizens of New York in general.

the event of a power outage or other catastrophic event.[2] The board should periodically review and update its IT policies to reflect the changes in technology or the computing environment.

IT Policies Are Not Adequate

The Board did not adopt adequate IT policies and procedures. While the District has a written acceptable use policy, the Board has not adopted policies and procedures for granting, changing and terminating user access rights to the District's network and financial application.

Additionally, District officials have not adopted policies and procedures for breach notification and have not developed a written disaster recovery plan. Although servers and financial data are backed up on a regular basis and backups are stored offsite, personnel have no guidelines to minimize the loss of equipment and data or implement data recovery in the event of a disaster.

Without comprehensive IT policies, users might not know how to appropriately use the District's network, devices and safeguard 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 the system and data by putting computers at risk for viruses or malicious software (malware).[3]

If PPSI is compromised and the District has not implemented a breach notification policy, employees responsible for safeguarding PPSI data might not understand or be prepared to fulfill their legal obligation to notify affected individuals. And without a formal disaster recovery plan, District employees may not be aware of where they should go, or how they will continue to do their jobs, during and after a disruptive event.

Cybersecurity Awareness Training Is Not Provided to District Employees

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;

2 Such as a fire, computer virus or an inadvertent employee action

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

- Limiting the type of PPSI collected, accessed or displayed to essential information for the function performed;
- Malicious software, virus protection and the dangers of downloading files and programs from the Internet;
- Password controls; and
- Restricting physical access to IT systems and resources which can help protect them from intentional or unintentional harm, loss or compromise.

District officials told us that employees are not provided or required to attend formal cybersecurity awareness training. However, employees are notified, by email from the Technology Coordinator, to immediate IT-related security concerns. Without formal security awareness training, District employees are more likely to be unaware of a situation which could compromise IT assets and security, which places the IT system at greater risk.

District Officials Did Not Disable Unnecessary User Accounts

Unnecessary accounts can be potential entry points for attackers and could be used to inappropriately access and view PPSI. Also, unnecessary user accounts create additional work when managing District network access. To decrease the risk of unauthorized access, it is imperative District officials disable unnecessary accounts as soon as the accounts are no longer needed.

The IT Department manages and maintains the District's networks and adds, removes and modifies user access from the network. We examined 330 enabled network user accounts[4] to determine whether they are in accordance with industry best practices and found:

- 52 user accounts (16 percent) belonged to employees who are no longer employed by the District. One of these previous employee accounts belonged to an individual who separated from the District in 2004.
- 43 generic accounts (13 percent) that are not associated with a unique individual. After our inquiry, District officials deleted 19 of these generic accounts.

We also examined 14 enabled local user accounts on the financial server to determine whether they are in accordance with industry best practices. We found two (14 percent) user accounts that should be disabled. One employee no longer works for the District and the other employee, although she works in the District office, has two unique user accounts and only needs one.

4 245 user accounts on the teacher/student active directory and 85 user accounts on the administrative active directory

District officials told us they have not implemented formal policies and procedures for granting, revoking and modifying individual access rights to the network and the financial server. Additionally, District officials told us no one earmarks unnecessary user accounts for disabling by comparing a master list of all active employees against all user accounts in the network. As a result, the District has unnecessary user accounts, which increase the risk of unauthorized access.

District Users Had Excessive Access to the Financial Application

Effective controls over access rights to the financial application should allow users access to those computerized functions that are consistent with their job responsibilities and should prevent users from being involved in multiple aspects of financial transactions. There should be written procedures in place for granting, changing and terminating access rights to the financial application software. These procedures should establish who has the authority to grant or change access and allow users to access only what is necessary to complete their job duties. District officials should ensure that user access rights are promptly adjusted or deactivated when employees' responsibilities change.

An individual who has financial system administrative rights can add new users, configure certain system settings, override management controls and create and change user access. Accordingly, financial system administrators should not be involved in the District's financial operation. If this is not feasible, then system activity should be periodically reviewed.

The District does not have any written procedures outlining how user access rights should be established or modified. As a result, District officials have improperly assigned administrative privileges and provided excessive access rights to the District's financial application.

The Assistant Superintendent is responsible for adding, removing and modifying user access rights to the financial system. Because he is responsible for overseeing the District's Business Office, he is not independent of the financial recordkeeping function. In addition, the District Treasurer (Treasurer) and IT technician, who has two user accounts, have administrative access rights. Therefore, the Assistant Superintendent, IT technician and Treasurer have unrestricted access to all functions within the financial application, including approving requisitions and modifying purchase orders, system configurations settings and employee earnings.

District officials told us the Treasurer does not need full access to the financial system. She was granted full access for a time period when the District did not have an Assistant Superintendent and her access has not been updated since that time. The IT technician told us he is unsure why he has two user accounts. As a result, due to improper assignment of administrative privileges and access rights, there is an increased risk that unauthorized changes to the accounting records, software security settings and user authorization privileges could occur

and go undetected. This could lead to the loss of important financial and PPSI data and could cause interruptions to District operations.

PPSI Data Is Not Properly Managed

The District collects and stores data received and produced from its operations, including PPSI, such as confidential employee data. Classifying the PPSI data can help identify the appropriate type of security controls for safeguarding that data.

District officials have not established a classification scheme for PPSI, and as a result, have not assigned a security level to the data. While District officials have knowledge of where certain PPSI is retained, they do not know the full extent to which PPSI resides on the electronic equipment used by District staff on a daily basis and they have not inventoried or classified the data based on risk. Unless District officials classify the data they maintain and set up appropriate security levels for PPSI, there is an increased risk that PPSI could be exposed to unauthorized users and efforts to properly notify affected parties in the event of a data breach could be hampered.

What Do We Recommend?

The Board should:

1. Adopt a written breach notification policy requiring that certain individuals be notified if there is a system security breach related to PPSI.
2. Develop and adopt a comprehensive written disaster recovery plan.
3. Adopt written IT policies to address adding, removing and modifying user access rights to the network, financial server and financial application.
4. Develop policies to address the classification and safeguarding of PPSI.

The Technology Coordinator and District officials should:

5. Develop detailed written procedures that supplement adopted IT policies.
6. Ensure employees receive formal IT cybersecurity awareness training on a periodic basis that reflects current risks identified by the IT community.
7. Evaluate all existing network and financial server user accounts, disable any deemed unnecessary and periodically review for necessity and appropriateness.
8. Periodically review and update user accounts and privileges on the financial application.
9. Inventory and classify PPSI to ensure it is appropriately safeguarded.

Appendix A: Response From District Officials

CAZENOVIA CENTRAL SCHOOL DISTRICT
CAZENOVIA, NEW YORK 13035-1098
Website: www.caz.cnyric.org

Matthew Reilly
Superintendent

(315) 655-1317
Fax (315) 655-1375

June 26, 2019

Rebecca Wilcox, Chief Examiner
Office of the State Comptroller, Syracuse Regional Office
State Office Building, Room 409
333 East Washington Street
Syracuse, NY 13202-1428

Ms. Wilcox:

This letter is written in response to the Office of the State Comptroller Audit for the period of July 1, 2017 through June 30, 2018 with the purpose of reviewing our control and handling of personal, private and sensitive information as well as access to our district financial system. We were presented with the Draft Audit Report on May 30, 2019 and subsequently held an exit interview on June 7, 2019.

We agree with the findings of the audit process. We agree that the facts relied upon in preparing the findings are accurate and complete. We agree with the recommendations provided in the draft report. We will soon prepare our Corrective Action Plan and will submit it after review and approval by the Board of Education.

District leadership and the technology department embraced the opportunity to take a closer look at the handling of sensitive data and our technological security systems. We appreciated the process and the efforts of the audit staff in identifying areas for improvement.

Using the key findings and recommendations of the audit report as a guide, it is our intention to take the measures necessary to further protect the district and its stakeholders. Moving forward, not only will we craft our corrective action plan and subsequent policy and procedural changes needed, but will maintain a higher level of diligence regarding our technology and data security.

In closing, we would like to thank the Senior Examiner assigned to our district and your office for your support during this process.

Sincerely,

Matthew Reilly, Superintendent

cc: Jan Woodworth, Board of Education
Thomas Finnerty, Assistant Superintendent
Janet Goris, District Clerk

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 reviewed the District's policy manual 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 the internal controls over IT.
- We interviewed officials to identify and gain an understanding of the roles and responsibilities of persons significant to maintaining the security of the District's IT assets.
- We interviewed officials and employees and reviewed certain District records to determine if employees received cybersecurity awareness training.
- We interviewed District employees to determine what safeguards were in place to protect sensitive data and financial assets.
- We assessed user access to the financial application to determine whether access to PPSI was reasonable and appropriate.
- We judgmentally selected a sample of 10 computers and reviewed web history reports for accessed websites that violated the District's acceptable use policy, to identify Internet use and pages that disclosed PPSI, or websites that were accessed that could put the District's network at risk. We selected all computers assigned to District and Business Office employees (nine computers) based upon risk and included computers used by employees with access to financial and employee records. Additionally, we selected the one computer assigned to the IT technician who has administrator access rights to the network, financial server and financial software application.
- We analyzed user accounts and security settings applied to those accounts on the financial server.
- We used active directory scripts to analyze and access the District's two active directories (administrative and teacher/student) to determine if user account and security settings were necessary and appropriate. We reviewed the user accounts and compared them to a list of current employees to identify inactive and unnecessary accounts.
- We observed and documented the physical security controls throughout the facilities.

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/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

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner

State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428

Tel (315) 428-4192 • Fax (315) 426-2119 • Email: Muni-Syracuse@osc.ny.gov

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

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