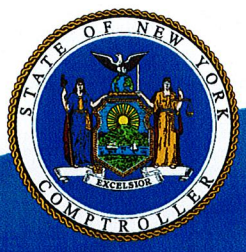
DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2019M-128

Belleville-Henderson Central School District

Information Technology

OCTOBER 2019



OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Belleville-Henderson Central School District

Audit Objective

Determine whether District officials ensured employees' personal, private, and sensitive information (PPSI) was adequately protected from unauthorized access, use and loss.

Key Findings

- District officials did not provide IT security awareness training to all employees.
- District officials did not develop procedures for managing, limiting and monitoring user accounts and permissions and securing personal, private and sensitive information.
- The District did not have a disaster recovery plan.

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

Key Recommendations

- Provide periodic IT security awareness training to all employees who use IT resources.
- Develop written procedures for managing access to the network and financial application.
- Develop and adopt a disaster recovery plan.

District officials agreed with our recommendations and indicated they had already taken or planned to take corrective action.

Background

Belleville-Henderson Central School District (District) has a single K-12 building and serves the Towns of Adams, Ellisburg and Henderson in Jefferson County.

The District is governed by a seven-member Board of Education (Board) that 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 day-to-day management of the District.

Quick Facts	
Employees	88
Student Enrollment	455
Desktop, Laptop and Tablet Computers	843
Total Network Accounts	1,176
Nonstudent Network Accounts	691

Audit Period

July 1, 2017 – September 30, 2018. We performed IT scans through November 1, 2018.

Information Technology

The District relied on its information technology (IT) assets for Internet access, email and maintaining financial records that may involve personal, private or sensitive information (PPSI).[1] The District contracted with the Mohawk Regional Information Center (MORIC) for Internet filtering; data privacy and security; network and software support, including support for its financial application; and the services of a network administrator.

The Network Administrator worked onsite at the District two days per week and was responsible for overseeing general computer system operations. Eight MORIC and six District employees had access to the District's financial application.

Why Should the District Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, District officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data and that communicates related policies and procedures to all employees. The training should center on emerging trends such as information theft, social engineering attacks[2] and computer viruses and other types of malicious software, all of which may result in PPSI compromise or expose the District to ransomware attacks. Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything that attendees need to perform their jobs.

The training should also cover key security concepts that include the dangers of downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections; and how to respond if a virus or an information security breach is detected.

The District Did Not Provide IT Security Awareness Training to All IT Users

During our audit period, the District did not provide all IT users with IT security awareness training to help ensure they understood security measures to protect

1 PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers (students), third parties or other individuals or entities.

2 Social engineering attacks are methods used to deceive users into revealing confidential or sensitive information.

PPSI. The Network Administrator sent out periodic emails[3] to keep employees informed about known or possible IT cyberattacks. But, this was not a sufficient substitute for formal IT security awareness training.

Also, the District had a written policy directing the Superintendent, or his or her designee, to provide staff with training in the proper and effective use of the District's computer system. However, we found that the District did not provide training to all users regarding proper usage of the IT infrastructure, software and data.

After we inquired about IT security awareness training during our fieldwork, District officials provided training on data security and privacy awareness in December 2018 to some employees. Two of the six users of the financial system attended this training, which covered concerns related to data security and password controls and provided an overview of email phishing. District officials should provide similar training to the remaining employees who use IT resources.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. District officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that users, or those who manage IT, understand the IT security policies and procedures and their roles and responsibilities related to IT and data security. Without periodic, formal security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, data and PPSI could be at greater risk for unauthorized access, misuse or abuse.

Why Should the District Manage User Accounts and User Permissions?

User accounts provide access to networks and financial applications and should be actively managed to minimize the risk of misuse. If not properly managed, user accounts could be potential entry points for attackers because they could be used to inappropriately access and view PPSI on the network and in the financial system. A district should have written procedures for granting, changing and revoking access rights to the network and to the financial application.

In addition, to minimize the risk of unauthorized access, district officials should regularly review enabled network user accounts to ensure they are still needed.

---

3 In October 2018, the Network Administrator sent out two emails. One warned staff of malicious emails that appeared to come from another staff member, but instead were coming from an attacker. The other informed staff of attempted impersonation attacks across the region in which attackers attempted to mislead District IT users by sending email to them from a fake user. The fake user's email address had a domain name of a known district after an actual user name in the email address (e.g., fake user name@legitimate district name.edu), which was designed to gain the trust of the email recipient.

Officials must disable unnecessary accounts as soon as there is no longer a need for them.

Because shared accounts are not assigned to a single user, officials may have difficulty managing these accounts and linking any suspicious activity to a specific user. To help ensure individual accountability, each user should have his or her own user account.

IT managers must set up user accounts with specific permissions needed by each individual to perform their job functions. This ensures access to PPSI is restricted to only those individuals who are authorized to access it. Also, officials should periodically monitor user permissions to ensure that employees have access to only those areas or data that they need for their job functions.

Officials Did Not Adequately Manage User Accounts and Permissions

District officials did not adequately manage user accounts and permissions for its network and financial application. As a result, we found that the District had unneeded and shared accounts that had not been disabled and/or monitored, and some District employees who had access to the financial application had excessive user permissions to employees' PPSI, as follows:

Former Employees – When new employees were hired, District officials provided the Network Administrator with a letter or form indicating the level of access that the new employees should be granted, so they could be given a network and/or financial application user account. However, the District did not have a formal process or written procedures for revoking user accounts.

Consequently, the Network Administrator disabled a former employee's network and/or financial application account only when he became aware that the employee had left District employment. During our review of all 691 nonstudent network accounts, we found four active network accounts of three former employees and one former Board member.

One of the former employees had left District employment in 2014. The former Board member left the District at the end of June 2018.[4] User accounts of former employees that have not been disabled or removed could potentially be used by those individuals or others for malicious purposes.

Unneeded Accounts – During our review of all 691 nonstudent network accounts, we found 12 accounts that had originally been created for various uses that were no longer needed, including one for vendors to use to send emails and two related to installing software.

4 The District did not have employment records for the remaining two employees: a former 4H employee and a former support staff member.

After we notified the Network Administrator of the existence of the unneeded accounts, he disabled them during our fieldwork. Officials must disable unnecessary accounts as soon as there is no longer a need for them.

Shared Accounts – During our review of all 691 nonstudent network accounts, we found three shared accounts. One was used in a lab room to show videos on a projector, one was used in the library on three computers to access the library's catalog and the third was used by all substitute teachers to access the District's student information system.

Although these shared accounts were needed accounts, the District did not have any procedures in place to monitor who used the accounts. As a result, the District has a greater risk that PPSI could be changed intentionally or unintentionally or used inappropriately and that officials would not be able to identify who performed the unauthorized activities.

Financial Application User Permissions – We reviewed permissions for all 14 users of the District's financial application (eight MORIC and six District employees) and found that four District users had unnecessary user permissions that allowed them to access PPSI, which they did not need to fulfill their roles and/or job duties. The unnecessary user permissions included the ability to add, delete and modify employee salaries, birth dates, addresses, retirement numbers and bank account information for employee's direct deposit accounts.

District officials did not have written procedures for granting, changing and revoking access rights to the District's network and financial application. In addition, officials did not regularly review user accounts to ensure they had appropriate user permissions. As a result, the 16 unneeded network accounts and unnecessary user permissions went unnoticed until our audit.

Because the District's network had unneeded active user accounts, it had a greater risk that these accounts could have been used as entry points for attackers to access PPSI and compromise IT resources. In addition, because District users of the financial application had unnecessary user permissions, the District has an increased risk that employees' PPSI could be used to commit fraud and/or identify theft and that it would be liable for losses incurred.

Why Should the District Have a Disaster Recovery Plan?

To minimize the risk of data loss or suffering a serious interruption of services, District officials should establish a formal written disaster recovery plan (plan). The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, computer virus or inadvertent employee action) that could compromise the network and the availability or integrity of the District's IT system and data, including its financial application and any PPSI contained therein. Typically, a

plan involves analyzing business processes, focusing on disaster prevention and identifying roles of key individuals and necessary precautions to take to maintain or quickly resume operations.

The District Did Not Have a Disaster Recovery Plan

The Board did not develop a formal disaster recovery plan as it relates to the IT environment to describe how officials would respond to potential disasters.

District officials told us that the financial data are backed up regularly, and backups are stored offsite. However, because the District does not have a plan that is specific to its IT environment, personnel have no guidelines to minimize the loss of IT equipment and data or implement data recovery in the event of a disaster.

Without a comprehensive plan, 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 State aid claims.

What Do We Recommend?

The Network Administrator and District officials should:

1. Provide periodic IT security awareness training to all District employees who use IT resources.
2. Develop written procedures for granting, changing and revoking access rights to the network and financial application.
3. Evaluate all existing network accounts, disable any deemed unnecessary and periodically review for necessity and appropriateness.
4. Assess user permissions for all user accounts of the financial application and remove excessive user permissions for those users who do not need that level of access to perform their job duties.

The Board should:

5. Develop and adopt a formal disaster recovery plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

Appendix A: Response From District Officials

Belleville Henderson Central School District

8372 County Route 75
Adams, NY 13605
www.bhpanthers.org

315 846-5411 Main Office
315-846-5825 Guidance Office
315-846-5826 District Office
315-846-5617 Fax

HOME OF THE PANTHERS

October 5, 2019

Rebecca Wilcox, Chief Examiner for NYSOSC
Syracuse Regional Office
State Office Building Room 409
333 E Washington Street,
Syracuse, NY 13202-1428

Dear Chief Examiner,

This letter is the District's response to the New York State Office of State Comptroller (NYSOSC) findings from an audit that the NYSOSC conducted in the Fall of 2018. The District concurs with NYSOSC findings and the District has expedited a response to address these matters. Since the NYSOSC Examiner's initial exit meeting, internet training was performed by highly qualified individuals in December 2018 and February 2019. The District did additional training on September 2, 2019. Trainings include proper use of the District's technology, best practices in the use of District email, and a clear understanding that illustrates how to identify phishing attacks. The District's policy and practice as in the past continues to be that all District employees review and accept the District's Acceptable Use Policy each time an employee signs in on a District computer or device.

The District's revised procedures will ensure that all employees are up to date on instructional technology (IT) policies, procedures and current threats. The procedures includes trainings for all staff on a monthly basis. Belleville Henderson School District has been short staffed in technology for many years. The Board is in complete support of a stronger plan for the management of internet technology. The 2019-2020 budget includes this development. The District has secured a highly qualified managed IT service.

The District removed all users in the winter of 2019 who should not have access to the network during the 2018-2019 school year. Permissions are set in accordance with employee's job duties and employment status with the district. The District is reviewing all procedures for granting, changing and revoking access rights to the network and financial applications. The District's plan will review user accounts quarterly to ensure these accounts are accurate.

The District reviews permissions for all user accounts on the financial applications and updates user permissions if there is a change in staff. In addition, the District has adopted a quarterly user access rights review process that permits the granting of rights when necessary provided it is consistent with fiscal internal controls.

The District is working with the Board of Education methodically to develop a Comprehensive Disaster Recovery Plan and a procedure to test this Disaster Recovery Plan. A Corrective Action Plan will follow within the allotted 90-day timeframe. Thank you for your audit of Belleville Henderson's Technology Systems.

Sincerely,

Jane A. Collins

Jane A. Collins

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 and MORIC personnel and reviewed District IT policies to gain an understanding of its IT environment, internal controls, disaster recovery plan and IT security awareness and other IT-related training.
- We used our professional judgment to review the computers assigned to six District users of the financial application. We chose these individuals because they had access to financial and employee records.
- We reviewed the user account permissions for all 14 users (eight MORIC employees and six District employees) of the financial application and determined whether they were appropriate based on job functions and required access to sensitive data.
- We ran computerized audit scripts and analyzed the reports produced to assess network user accounts and security settings applied to those accounts. We reviewed user accounts and compared them to the current employee list to identify inactive and unneeded accounts.

Our audit also examined the adequacy of certain information technology 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 District 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