REPORT OF EXAMINATION | 2019M-121

Evans-Brant Central School District

Information Technology

OCTOBER 2019

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

Contents

Report Highlights

Evans-Brant Central School District

Audit Objective

Determine whether information technology (IT) assets are properly safeguarded, secured and accessed for appropriate District purposes.

Key Findings

- District officials did not provide IT security awareness training for individuals who used District IT assets.
- Personal Internet use was found on computers assigned to four employees who routinely accessed personal, private and sensitive information (PPSI).

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

Key Recommendations

- Provide periodic IT security awareness training.
- Provide adequate oversight of employee Internet use to ensure it complies with Board policies and regulations.

District officials agreed with our findings and recommendations and indicated they planned to initiate corrective action.

Background

The Evans-Brant Central School District (District) serves the Towns of Brant, Evans and Eden in Erie County and the Cattaraugus Reservation of the Seneca Nation of Indians.

The District is governed by an elected seven-member Board of Education (Board). The Superintendent of Schools is the chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The District employs a Director of Technology/Chief Information Officer (Director) to manage its IT department.

Quick Facts	
Total Network Accounts	2,860
Employee Network Accounts	433
Employee Computers Examined	26

Audit Period

July 1, 2017 – May 15, 2019

Information Technology

Why Should District Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI,[1] District officials should provide periodic IT security awareness training. This training should explain the proper rules of behavior for using the Internet, IT systems, data and PPSI and communicate related policies and procedures to all individuals using them. 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. 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 District's acceptable use policy (AUP) and corresponding regulations for employees and students states that IT users must receive training on the proper use of its IT environment. In addition, the AUP also indicates that use of the District's computer system for personal reasons is strictly prohibited.

IT Users Are Not Provided With Cybersecurity Training

During our audit period, the District did not provide formalized IT security awareness training to employees or students. Officials told us that school librarians offered a "digital citizenship class" to 8th grade students annually and employees were given updates and cybersecurity information through District emails. However, organized IT security awareness training was not provided.

Without IT 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 a greater risk for unauthorized access, misuse or loss.

How Does an Acceptable Use Policy Protect IT Assets?

Acceptable use policies describe what constitutes appropriate and inappropriate use of IT resources, along with the Board's expectations concerning personal use of IT equipment and user privacy.[3] Monitoring compliance with the acceptable use policy involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity.

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

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

3 For example, management may reserve the right to examine email, personal file directories, web access and other information stored on computers, at any time and without notice.

Officials should monitor and analyze activities for signs of possible violations or imminent threats of violations of IT security policies, AUPs or standard security practices. Automated mechanisms may be used to help perform this process and can assist security professionals to routinely assess computer security, perform investigations during and after an incident and even recognize an ongoing attempt of unauthorized access.

The District's AUP and corresponding regulations state that the District's computer system should be used only for school-related work or activities and may not be used for any illegal purpose. Use of the computer system for personal reasons is strictly prohibited. Also, employees and authorized users are not allowed to access any personal email accounts.

The AUP establishes the District's right to monitor and review each employee's computer, email and Internet use and advises employees that they should not expect privacy when using the computer system. Annually, employees are given a copy of the AUP and are required to review, sign and return it to the District.

Some District Computers Were Used for Personal Activities

We found evidence that some employees did not comply with the AUP. We reviewed the web browsing history on 26 computers[4] and found significant personal Internet use on four computers. This included personal shopping, banking and email use; social networking; web searches for non-District related subjects; and filing personal income tax returns. In addition, we found evidence of inappropriate and other questionable Internet use on one of the four computers that was assigned to a member of the District's administrative staff. The employee used the computer to access multiple websites of a personal, nonbusiness or otherwise high-risk nature.

All four of the employees using these four computers signed the AUP and performed job duties that involved routinely accessing PPSI. As a result, their personal Internet use unnecessarily exposed this information to possibly being compromised.

District officials were unaware of this personal and inappropriate computer use because they did not routinely monitor employee Internet use for AUP compliance. In addition, some employees were able to access their personal email accounts using District computers because their email accounts were hosted by the same provider the District used for its employee email accounts. This prevented the personal email accounts from being blocked on the District's network.

4 Out of 26 computers we scanned, no or limited web browser history was exported from 11 computers. District officials indicated that it may have resulted from the users not using the Internet or because they deleted the web history. Refer to Appendix B for information on our sample selection.

However, just because employees could access their personal email accounts while on the District's network did not mean that they were allowed to do so. This use was not in accordance with the District's AUP.

Internet browsing and personal email use increases the likelihood of computers being exposed to malicious software that may compromise PPSI. As a result, the District's IT assets and any PPSI they contain have a higher risk of exposure to damage and PPSI breach, loss or misuse.

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 financial system and any PPSI contained therein. Typically, a plan involves analyzing business processes and continuity needs, focusing on disaster prevention and identifying roles of key individuals and necessary precautions to take to maintain or quickly resume operations.

The Board and District Officials Have Not Established a Disaster Recovery Plan

The Board did not adopt a comprehensive written plan to describe how officials would respond to potential disasters.

The District contracted with Erie 1 BOCES[5] (BOCES) for certain IT support services. One of the services related to school district disaster recovery planning – which costs approximately $12,000 annually – included providing a plan template and assistance to help refine the plan for specific school district needs. However, the District did not use this service.

The Director told us he was not aware of this service. Without a formal written plan, the District has an increased risk that it could lose important data and suffer serious interruption in operations.

What Do We Recommend?

The Board should:

1. Ensure that officials monitor employee compliance with the AUP.
2. Adopt a written disaster recovery plan.

5 Board of Cooperative Educational Services

3. Ensure BOCES provides all services that the District has contracted for, specifically a disaster recovery plan template and assistance to help refine the plan for the District's needs.

The Director and District officials should:

4. Provide, or coordinate the provision of, periodic IT cybersecurity awareness training to individuals who use District IT resources.

5. Monitor personal computer and Internet use to ensure employees comply with the AUP and corresponding regulations.

Appendix A: Response From District Officials

LAKE SHORE CENTRAL SCHOOLS

EVANS-BRANT CENTRAL SCHOOL DISTRICT

DISTRICT OFFICE: 959 BEACH ROAD, ANGOLA, NEW YORK 14006-9782

On Beautiful Lake Erie

All Schools 716-549-2300
Fax 716-549-6407
www.lakeshorecsd.org

SENIOR HIGH
959 BEACH ROAD
ANGOLA, NY 14006-9782
716-926-2307
FAX 716-549-4033

MIDDLE SCHOOL
8855 ERIE ROAD
ANGOLA, NY 14006-9624
716-926-2400
FAX 716-549-4374

ANTHONY J. SCHMIDT
9455 LAKE SHORE ROAD
ANGOLA, NY 14006-9400
716-926-2350
FAX 716-549-4428

HIGHLAND
6745 ERIE ROAD
DERBY, NY 14047-9698
716-926-2460
FAX 716-947-9269

JOHN T. WAUGH
100 HIGH STREET
ANGOLA, NY 14006-1300
716-926-2370
FAX 716-549-2380

TRANSPORTATION
8710 N. MAIN STREET
ANGOLA, NY 14006-9603
716-926-2240
FAX 716-549-4369

W. T. HOAG EDUC. CENTER
42 SUNSET BOULEVARD
ANGOLA, NY 14006-1000
716-926-2480
FAX 716-549-4391

September 25, 2019

Office of the State Comptroller
Buffalo Regional Office
295 Main Street – Suite 1032
Buffalo, NY 14203-2510

Dear Sir/Madam:

We are in receipt of your draft report of the State Comptroller's Office audit of the Evans-Brant Central School District for the period July 1, 2017 – May 15, 2019. The District Board of Education and Administration strive for a culture of strict accountability and transparency, and appreciate your auditors' efforts to examine the District's Information Technology control structure and provide the District with its recommendations for suggested improvements. We are writing to provide you with the District's response to the findings recommendations contained in your report, and to provide you with the District's corrective actions in response to the findings and recommendations. We concur with all of the findings and recommendations outlined in your report, and will address the findings and our corrective actions in the same order that the findings and recommendations appear in your report.

Recommendations:

1. *"The Board should ensure that officials monitor employee compliance with the AUP."*

Although the District requires employees and students to sign an annual acknowledgement of the District's AUP, the auditors noted that the District should monitor compliance. The District agrees that monitoring compliance with the AUP will help ensure that the District's technology resources are not being misused by staff. The Board will direct the administrative staff and IT department employees to develop and implement a plan to monitor employee compliance with the District's AUP.

2. *"The Board should adopt a written disaster recovery plan."*

The District agrees with this finding and recommendation. While the District follows current IT standards for back-up and off-site storage of critical IT information, it recognizes that it does not have a written disaster recovery plan that outlines the procedures to be followed if needed. The District's Director of Technology will work with the Assistant Superintendent for Administration

and Finance to document the steps to be followed in the event that the District experiences a loss of data and/or program access due to a disaster. The disaster recovery plan will also include procedures to be followed by the Western New York Regional Information Center staff at Erie 1 BOCES for technology applications housed by the BOCES. The District will investigate a service offered by the WNYRIC that would assist the District in developing a formal written disaster recovery plan. Once the District's disaster recovery plan is developed, it will be presented to the Board of Education for formal adoption.

3. *"The Board should ensure BOCES staff provides all services that the District has contracted for, specifically a disaster recovery plan template and assistance to help refine the plan for the District's needs."*

The Board will instruct District Administration including the Director of Technology to review the District's annual purchased services from BOCES, with special emphasis on IT services purchased from the WNYRIC/Erie 1 BOCES. The District's Administration will schedule a meeting with the District's representative from Erie 1 BOCES during preparation of the District's annual operating budget so that any adjustments to the purchased services will be reflected in the District's budget for the ensuing year. Additionally, District Administration will gain assurance from the Director of IT and the BOCES Representative that all purchased services are being provided to the District.

4. *"The Director and District officials should provide, or coordinate the provision of, periodic IT cyber security awareness training to individuals who use District IT resources."*

The Director of Technology is working with other District administrators and the vendor that provides the District's mandated annual training and refresher courses. The vendor ([redacted]) offers the District free online training courses in a wide variety of subjects, and the District utilizes the service to provide required annual staff training for "Right to Know", "Sexual Harassment", "Anti Bullying and Violence Prevention" and other topics. The addition of a cyber security awareness training course to the current offerings would provide the District the ability to assign it to staff as a required training course. Since the online courses offered include an exam to be completed by the employee and documentation of course completion, the District will be able to insure that all staff members have completed the annual required training. Additionally, the District will utilize its two Technology Integrators to work with classroom teachers and other District employees to safeguard against cyber security threats by making sure District protocols like locking computer screens when the employee is away from the device to protect the security of student and District data, and informing staff of threats that can be encountered when dealing with the District's IT network and the World Wide Web.

5. *"The Director and District Officials should monitor personal computer and Internet use to ensure employees comply with the AUP and corresponding regulations."*

In response to this recommendation, the District will work to implement random computer audits throughout each school year to check District owned computers for viruses and/or malware, unsupported and non-District provided software and applications and physical damage. Additionally, the random audits will also review internet browsing history to insure that the District's computers are not being inappropriately utilized for non-business functions. The

audits will use a random sampling of computer hardware issued to teachers and other staff members from the District's various work locations. District IT staff will review [redacted] files to review internet browsing history, and will review [redacted] files to review email use for the prior 30 day period, with the examination period extended if necessary due to any findings. Findings of the random audits will be reviewed with the employee, and any unauthorized software or applications will be removed through reimaging of the device to update it to the latest operating system and antivirus software.

We believe this corrective action plan will address the findings in the audit. Thank you again for your efforts in helping the District improve its internal control structure and for the courtesies extended to our staff by your auditors during the completion of the audit work.

Sincerely,

Charles A. Galluzzo, Ed.D.
Superintendent

Daniel W. Pacos
Assistant Superintendent for
Administration & Finance

Jeffrey T. Barnes
Technology Director

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 our audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed Board policies, regulations and minutes and District procedures relating to IT operations and assets and interviewed District officials to obtain an understanding of the IT environment.
- We interviewed District officials to determine whether employees and students received IT security awareness training and regularly reviewed the AUP.
- We used the master payroll list of 699 employees and our professional judgement to select a sample of 26 employees who likely accessed student, staff and financial PPSI. We reviewed the web browsing history on the computers assigned to these employees and evaluated whether their Internet use was in compliance with the AUP.
- We provided the Director with a computerized audit script to run and asked him to copy the reports and files generated by the script from our sample of 26 employees for us. We analyzed the reports and files, including Internet browsing histories, looking for potential issues related to personal and high-risk activities.

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 generally accepted government auditing standards (GAGAS). 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

BUFFALO REGIONAL OFFICE – Jeffrey D. Mazula, Chief Examiner

295 Main Street, Suite 1032 • Buffalo, New York 14203-2510

Tel (716) 847-3647 • Fax (716) 847-3643 • Email: Muni-Buffalo@osc.ny.gov

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming counties

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