REPORT OF EXAMINATION | 2019M-14

Ellicottville Central School District

Information Technology

JUNE 2019

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

Contents

Report Highlights

Ellicottville Central School District

Audit Objective

Determine whether the District ensured information technology (IT) assets were properly safeguarded and secured.

Key Findings

- District officials did not provide IT security awareness training for individuals who used District IT assets.
- Employees accessed websites for social networking, shopping, travel and other personal use.

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.

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

Background

The Ellicottville Central School District (District) serves the Towns of East Otto, Ellicottville, Franklinville, Great Valley, Humphrey and Mansfield in Cattaraugus County.

The District is governed by an elected seven member Board of Education (Board), which is responsible for establishing policies and procedures for all aspects of the District's IT environment. The Superintendent of Schools (Superintendent) 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.

Quick Facts	
Student Network Accounts	557
Employee Network Accounts	111
Desktops, Laptops and Tablets	1,143
Servers	4

Audit Period

July 1, 2016 – December 18, 2018

Information Technology

The District relied on its IT systems for Internet access, email and maintaining and accessing personal, private and sensitive information (PPSI),[1] including financial, personnel and student records. The District employed a Technology Coordinator and a technical support specialist to manage its IT environment. The District also contracted with Erie 1 BOCES (BOCES) for hosting its firewalls and servers, providing IT support for these services and providing web-based IT security awareness training resources.

Why Should District Officials 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 user behavior for using the Internet and IT systems and data. The training should communicate related policies and procedures to all employees and students and 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 training should also cover key security concepts such as the dangers of downloading files and programs from the Internet or portable devices such as thumb drives; the importance of selecting strong passwords; any requirements related to protecting PPSI; the risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected. The District's acceptable use policies (AUPs) for employees and students state that the Superintendent should provide IT users with training in the proper and effective use of the District's IT environment.

IT Users Were Not Provided With IT Security Awareness Training

During our audit period, the District did not provide any IT security awareness training. The Technology Coordinator told us that the District relied on BOCES to provide updates and information related to IT environments and cybersecurity. However, during our audit period, the District did not use the BOCES web-based IT security awareness training resources.

1 Personal, private and sensitive information (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, students, third parties or other individuals or entities.

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

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 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.

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

The District's AUP states that personal use of IT resources by employees is permitted on a limited basis. The AUP establishes the District's right to monitor, review and audit each employee's computer and Internet use. Therefore, employees should not expect privacy when using the system. On an annual basis, District employees are given a copy of the AUP and are required to sign a computer use agreement.

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 15 computers[4] and found significant personal Internet use on three computers. This included personal shopping and email use, social media use, web searches for travel and other Internet browsing of a personal nature.

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.

4 Refer to Appendix B for further information on our sample selection. We could not examine personal Internet use on one of the 15 computers because the employee cleared his web browsing history before our scan.

All three employees' job duties included routinely accessing PPSI. As a result, their personal Internet use unnecessarily exposed this information to being compromised.

District officials did not routinely monitor employee Internet use for AUP compliance. The Superintendent told us he was aware of employees' personal use on District computers and the network because the District allows personal use when necessary, or when personal use for activities such as social media and personal email occurs during breaks or after work hours.

However, Internet browsing 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.

What Do We Recommend?

The Board should:

1. Ensure that officials periodically monitor employee compliance with the AUP.

The Technology Coordinator and District officials should:

2. Provide, or coordinate the provision of, periodic IT security awareness training to students and employees who use District IT resources.

3. Monitor Internet use to ensure employees comply with the AUP and Board policies.

Appendix A: Response From District Officials

ELLICOTTVILLE
Central School

5873 Route 219 • Ellicottville NY 14731
District: 716.699.2368 • MS/HS:716.699.2316 • Elementary 716.699.2318
www.eville.wnyric.org

May 8, 2019

Office of the State Comptroller
Attn. Jeff Mazula
295 Main Street, Room 1032
Buffalo, New York 14203-2510

Office of the State Comptroller,

The Ellicottville Central School District is in receipt of the NYS Comptroller's recent audit report for Information Technology (IT). In general, we acknowledge the "Key Findings" and "Key Recommendations" contained in the report. As a result, over the next few weeks, we, as a District, will review, discuss and consider necessary changes as appropriate. The District will then provide Corrective Action Plans as warranted and submit them to your office in a timely manner.

Sincerely,

Robert R. Miller, Superintendent
Ellicottville Central School

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, we performed the following audit procedures:

- We reviewed Board policies 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 received IT security awareness training or regularly reviewed AUPs.
- We judgmentally selected to review the web browsing history of nine employee user accounts[5] and the 15 computers and computing devices assigned to these individuals to evaluate whether their Internet use was in compliance with the AUP. We selected the nine employees for our sample based on job titles that indicated duties likely to involve accessing student, staff and financial PPSI. We chose to review the following titles and individuals: Superintendent, School Business Official, Technology Coordinator, technical support specialist, accounts payable clerk/guidance secretary, payroll clerk/tax collector and three randomly selected teachers.
- We provided the Technology Coordinator with a computerized audit script to run and asked her to copy the reports and files generated by the script for us from our sample of nine employee user accounts and the 15 computers assigned to these individuals. 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

5 From a population of 111 employee user accounts

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