REPORT OF EXAMINATION | 2019M-10

Hamburg Central School District

Information Technology

JULY 2019

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

Contents

Report Highlights

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

District officials generally agreed with our recommendations and indicated they planned to initiate corrective action. Appendix B includes our comment on the District's response.

Background

The Hamburg Central School District (District) serves the Towns of Boston, Eden, Hamburg and Orchard Park in Erie County.

The District is governed by an elected seven-member Board of Education (Board). 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.

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

Quick Facts	
Employee Network Accounts	631
Student Network Accounts	3,707
Employee Computers Examined	15

Audit Period

July 1, 2017 – September 11, 2018

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 cybersecurity 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 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 policy (AUP) and corresponding regulations for employees and students indicates that IT users must receive training on the proper use of its IT environment.

IT Users Are Not Provided With Cybersecurity Training

During our audit period, the District did not provide any cybersecurity awareness training to employees or students. Officials told us that students learned about cybersecurity through various classes, such as health and career classes, and employees were given updates and cybersecurity information through District emails. However, organized cybersecurity awareness training was not provided.

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 cybersecurity 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.

---

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, 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.

How Does an Acceptable Use Policy Protect IT Assets?

The AUP and corresponding regulations state that computers are issued for school-related purposes and that personal use should be incidental and not interfere with employees' job duties and performance, must not violate any rules established by the AUP and must not damage hardware, software or communications systems.

The regulations prohibit the use of Internet games, web chats, unauthorized software and instant messaging. They define unacceptable use to include illegal or malicious use, use that disrupts the work of others, use for private business purposes and downloading music, games and other material.

Incidental personal email use is allowed, but must not interfere with job performance. Excessive personal use could result in disciplinary action. 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. Upon employment, 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 history on 15 computers[3] and found significant personal Internet use on four computers.[4] This included personal shopping and banking, web searches for non-District related subjects, social media use and personal email use.

All four employees' job duties included 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 computer use because they did not routinely monitor employee Internet use for AUP compliance. In addition, the Director told us he was not concerned with employees accessing personal email on District computers or its network because he thought the District's email filtering system and firewalls would catch any phishing schemes.

However, the email filtering system would only prevent phishing emails from being sent through the District's email system. It would not prevent phishing emails from being sent to employees' personal email accounts and being opened while using

3 Refer to Appendix C for further information on our sample selection. We were unable to examine Internet use on one of the 15 computers (the Director's) because he had cleared his web browsing history to access a webinar that was held the day that we scanned the computer.

4 The four computers were assigned to the Assistant Superintendent for Administration and Finance, Human Resources Manager, payroll clerk and Athletic Director.

the District's computers, thereby possibly infecting those computers and/or the District's network.

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.

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 Board of Cooperative Educational Services (BOCES) for certain IT support services. One of the services related to school district disaster recovery planning – which cost approximately $15,000 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 previously asked BOCES for a template and assistance with creating a plan, but BOCES did not provide any template or guidance. 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 and student compliance with the AUP.

2. Adopt a written disaster recovery plan.

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 employees and students who use District IT resources.

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

Appendix A: Response From District Officials[5]

Hamburg Central School District

Business and Transportation Office
Administration Building
5305 Abbott Rd.
Hamburg, NY 14075-1699
Telephone: (716) 646-3200 FAX: (716) 646-3209

Mr. Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
Buffalo Regional Office
295 Main Street, Suite 1032
Buffalo, New York 14203

June 3, 2019

Dear Mr. Mazula,

Please accept this letter as the District's response to preliminary draft findings as well as our Corrective Action Plan for the audit of the Hamburg Central School District, report no.'s 2019M-10 and 2019M-11.

Audit Recommendation 1:
Ensure that officials monitor employee and student compliance with the AUP.

Implementation Plan of Action:
A procedure will be developed to more closely monitor student and employee compliance with the AUP.

Implementation Date:
Fiscal year 2019-20

Person Responsible for Implementation:
Mr. Brent Jordan

Audit Recommendation 2:
Adopt a written disaster recovery plan.

Implementation Plan of Action:
A Disaster Recovery Plan will be developed and adopted by the Board of Education

Implementation Date:
Fiscal year 2019-20

Person Responsible for Implementation:
Mr. Brent Jordan

Audit Recommendation 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.

Implementation Plan of Action:
The District is in agreement that a comprehensive Disaster Recovery Plan should be developed and adopted by the Board of Education. The District is in the process of developing such a plan which will be board approved when completed. A point of clarification however, regarding the District's participation in Erie 1 BOCES coser for disaster recovery planning. Coser 650.950 is an annual, mandatary fee which contributes to the costs related to continued development and expansion of the secure/reliable technical

5 The District's response also addresses findings and recommendations from a separate report of the District that we released, titled *Hamburg Central School District – Continuing Education (2019M-11)*. This audit report can be found at: https://www.osc.state.ny.us/localgov/audits/index.htm. The first five recommendations refer to the current audit report and the last four refer to the separate report.

infrastructure demand required for today and into the future. The use of the service includes more than just a Disaster Recovery template, these services include but are not limited to:

- Continued refinement of WNYRIC's Disaster Recovery Plan and the testing of this plan through the COOP.
- Continued investment and contracted maintenance for enhancements of WNYRIC's main and alternate, redundant network/server room sites in the event of a disaster.
- Continued investment and contracted maintenance for enhanced monitoring tools necessary to ensure availability of WNYRIC's network.
- Investment and contracted maintenance in tools which provide redundancy and recovery of key WNYRIC infrastructure components.
- WNYRIC Service Desk support and the availability of key WNYRIC staff.
- Expanded security assistance with FBI and InfraGard involvement against security threats, illegal activity and AUP violations.
- WNYRIC Data recovery planning and testing in case of an incident or a disaster at one of WNYRIC's sites.
- Technologies which allow critical WNYRIC staff secure access to key technologies from anywhere on any device.
- Availability upon request of a Disaster Recovery Plan template for school districts to utilize and customize for their needs.

Although the Disaster Recovery Plan template is listed as a 2018-19 available service, until further inquiry by our District, it was not available to be provided. The District has been successful in procuring the template as of May, 2019.

Implementation Date:
Fiscal year 2019-20

Person Responsible for Implementation:
Mr. Brent Jordan

Audit Recommendation 4:
Provide, or coordinate the provision of, periodic IT cybersecurity awareness training to employees and students who use District IT resources.

Implementation Plan of Action:
Required training will be provided to staff and students via an email invitation. Compliance will be monitored and reported to the IT Director.

Implementation Date:
September, 2019

Person Responsible for Implementation:
Mr. Brent Jordan

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

Implementation Plan of Action:
The District's Acceptable Use Policy and corresponding Regulations state that computers are issued for school-related purposes and that personal use should be incidental and not interfere with employees' job duties and performance. Incidental personal email is allowed, but also must not interfere with job performance. It is the District's determination that employee use is incidental, and does not interfere with job performance. Moreover, the District's email filtering system and firewalls provide security to the

See Note 1 Page 10

network. As a part of our new cyber security training, staff and students will be educated on phishing schemes.

Implementation Date:
Not Applicable

Person Responsible for Implementation:
Not Applicable

Audit Recommendation 6:
Develop and adopt written policies and procedures for collecting, processing, recording and depositing cash receipts.

Implementation Plan of Action:
The District will develop and adopt written departmental policies and procedures for collecting, processing, recording and depositing cash receipts.

Implementation Date:
Fiscal year 2019-20

Person Responsible for Implementation:
Ms. Barbara Sporyz

Audit Recommendation 7:
Ensure that Department duties are adequately segregated or implement compensating controls such as increased supervisory review of the Department's work and a periodic reconciliation of the Department's cash receipts activity by someone independent of the Departments cash receipts process such as the Treasurer.

Implementation Plan of Action:
The District will designate only one individual to update class lists. The District Treasurer will reconcile the individual class lists on a periodic basis against bank statements (actual receipts).

Implementation Date:
September, 2019

Person Responsible for Implementation:
Ms. Barbara Sporyz

Audit Recommendation 8:
Issue press-numbered, duplicate receipts for all money collected and obtain a receipt from the business Office for all money remitted for deposit.

Implementation Plan of Action:
The Continuing Education Department will be directed to use press-numbered, duplicate cash receipt books for all funds received. A receipt is currently issued and provided to the individual for entering cash receipts into our accounting system. A copy of the receipt will be provided to the Continuing Education Department for all money remitted for deposit.

Implementation Date:
September, 2019

Person Responsible for Implementation:
Ms. Barbara Sporyz

Audit Recommendation no. 9:
Remit cash receipts in a timely manner to the Business Office for deposit, and do so in the same form and amount as received.

Implementation Plan of Action:
The Continuing Education Department will be directed to submit all deposits and corresponding receipts with supporting documentation on a daily basis.

Implementation Date:
September, 2019

Person Responsible for Implementation:
Ms. Barbara Sporyz

Sincerely,

Barbara S. Sporyz
Assistant Superintendent of Administrative Services & Finance

cc: Mr. Michael Cornell, Superintendent of Schools
Hamburg Central School District Board of Education

Appendix B: OSC Comment on the District's Response

Note 1

While the District's email filtering system and firewalls provide some security to the network, an email filtering system does not address the risk of using District computers to access personal email. Further, firewalls would not prevent malicious content on the Internet from reaching a District computer when that content is requested by the user (intentionally or inadvertently) or when the computer is not connected to the network.

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 our audit objective[6] 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 received IT cybersecurity awareness training and regularly reviewed acceptable use policies.
- We reviewed 15 employees' web browsing history on the 15 computers assigned to them to evaluate whether their Internet use was in compliance with the AUP. We judgmentally selected the 15 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; Assistant Superintendent for Administration and Finance; Director of Technology; District Treasurer; Director of Health, Physical Education and Recreation; Human Resources Manager; Maintenance Mechanic Crew Chief; community relations coordinator; high school nurse; payroll clerk; curriculum coordinator; webpage manager; and one teacher from each of the three District buildings.
- 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 15 employee user accounts 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.

6 We also issued a separate audit report, *Hamburg Central School District – Continuing Education (2019M-11).*

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 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/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