REPORT OF EXAMINATION | 2019M-13

Stockbridge Valley Central School District

Information Technology

JUNE 2019

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

Contents

Report Highlights

Stockbridge Valley Central School District

Audit Objective

Determine whether the Board and District officials established information technology (IT) policies and procedures to adequately safeguard personal, private and sensitive information (PPSI).

Key Findings

- Employees did not comply with the District's acceptable use policy (AUP).
- District officials did not disable unneeded user accounts in a timely manner.
- District officials did not provide IT security awareness training to employees.

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

Key Recommendations

- Monitor employees' computer use to ensure compliance with the AUP.
- Disable user accounts as soon as they are no longer needed.
- Provide employees with periodic IT security awareness training.

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

Background

The Stockbridge Valley Central School District (District) has a single K-12 building that is located in the Village of Munnsville in Madison County.

The District is governed by a seven-member Board of Education (Board) that is responsible for the general management and oversight 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 District's day-to-day management.

Quick Facts	
Student Enrollment	432
Employees	143
Employee Network Accounts	184
Desktops, Laptops and Tablets	572

Audit Period

July 1, 2017 – June 30, 2018

We extended our scope period forward to August 16, 2018 to perform IT scans.

Information Technology

The District relies on its 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] The District's technology coordinator was responsible for managing the District's IT resources.

The District contracted with Madison-Oneida Board of Cooperative Educational Services (BOCES) for library automation, computer service management and instructional technology. The District also contracted with the Mohawk Regional Information Center (MORIC) for maintaining the District's offsite backups and providing antivirus and firewall protection, Internet traffic filtering, software support and the services of a network technician.

How Does an Acceptable Use Policy Protect IT Assets and PPSI?

A school district should have acceptable computer use policies that define the procedures for computer, Internet and email use. The policies also should describe what constitutes appropriate and inappropriate use of IT resources and the board's expectations concerning personal use of IT equipment and user privacy. 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.

Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability. District officials can reduce the risks to PPSI and IT assets by monitoring Internet usage and by configuring web filtering software to block access to unacceptable websites and help limit access to sites that comply with the acceptable use policy. The District's acceptable use policy (AUP) prohibited the use of District computers for inappropriate,[2] obscene and illegal actives.

1 PPSI is any information to which unauthorized access, disclosure, modification, destruction 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 The District's acceptable use policy defined inappropriate use as a violation of the intended purpose of the network.

Officials Did Not Monitor Compliance With the Acceptable Use Policy

We found evidence that some employees did not comply with the AUP. We reviewed the Internet browsing histories on 10 employee computers and found evidence of inappropriate personal use on six computers.[3] This included online shopping and banking, personal email access, social media use and browsing travel, news and other entertainment websites.

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

The District's web filtering software blocked users from accessing websites that the AUP deemed inappropriate, obscene or illegal. However, officials did not monitor employee Internet use for inappropriate activity that was not automatically blocked by the software because the technology coordinator believed the filters were sufficient to block unsuitable websites.

As a result, employees engaged in inappropriate computer use that increased the likelihood of their computers being exposed to malicious software. Consequently, the District's IT assets and any PPSI they contained had a higher risk of exposure to damage and PPSI breach, loss, and misuse.

Why Should the District Manage User Accounts and Permissions?

Network and user application accounts are potential entry points for attackers because they could be used to inappropriately access the network and view PPSI in financial system and educational applications. A district should have written procedures for granting, changing and revoking network accounts and user application accounts for specific software applications.

In addition, to minimize the risk of unauthorized access, district officials should regularly review enabled network and user application accounts to ensure they are still needed. Officials must disable unnecessary accounts as soon as there is no longer a need for them.

Because generic 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.

Network accounts with administrative permissions have complete control of the network and can perform activities such as installing software, creating user

3 Refer to Appendix B for information on our sample selection.

accounts and manipulating security settings. Therefore, officials must ensure that network accounts with administrative permissions are assigned only to those who need them to perform their job duties.

Officials Did Not Adequately Manage User Accounts and Access

The District's AUP states that the Superintendent "shall remain the final authority on the issuance of network accounts," and that "staff who leave the District's employment may not maintain a network account." However, the District did not have written procedures for granting, changing and revoking network accounts and user application accounts for student information and financial software applications.

When new employees were hired, District officials filled out a form to define the type of access that should be given to the new employees, including network accounts and user application accounts for specific software applications. The technology coordinator then created the requested new user accounts. However, because the District did not have written procedures, the technology coordinator depended on officials' verbal requests for removing or inactivating user accounts when employees left District employment.

During our review of the 184 enabled employee network accounts, we found that two belonged to former employees, one of whom had left District employment in 2017. We also found 11 generic accounts that the technology coordinator told us were unnecessary.

In addition, we found that two employee network accounts had unnecessary administrative permissions. After we notified District officials of the existence of the unneeded accounts and those with excessive user permissions, they told us they deleted or disabled the two former employees' accounts and the 11 unnecessary generic accounts and removed the unneeded administrative permissions from the other two accounts.

Because the District did not have formal procedures for revoking access rights and regularly reviewing enabled user accounts, the unneeded user accounts and permissions went unnoticed until our audit. In addition, because the District's network had unused, 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.

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 communicates related policies and procedures to all employees and students. The training should center on emerging trends such as information theft, social engineering attacks[4] 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; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected.

District Employees Were Not Provided With IT Security Awareness Training

The District did not provide users with IT security awareness training to help ensure they understood security measures to protect PPSI. Officials told us they provided employees with verbal and written directives on how to address specific IT threats when BOCES communicated this information to the District. However, officials did not provide users with periodic, formal IT security awareness training that explained how users should comply with IT policies and procedures and proper rules of behavior for using District IT systems and data.

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 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 greater risk for unauthorized access, misuse or abuse.

What Do We Recommend?

District officials should:

1. Monitor employees' computer use to ensure compliance with the District's AUP.

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

2. Develop policies and procedures to ensure that unneeded user accounts are disabled in a timely manner and that all users have appropriate network permissions.

3. Periodically review network user accounts and disable those that are unneeded.

4. Ensure that employees receive formal IT security awareness training on an ongoing basis that reflects current risks identified by the IT cybersecurity community.

Appendix A: Response From District Officials

STOCKBRIDGE VALLEY
CENTRAL SCHOOL DISTRICT
"WE EMPOWER STUDENTS THROUGH EDUCATION"

BOARD OF EDUCATION
Barbary Reaves, President
Niki Maiura, Vice President
Pete Burke
Kristin Guinto
Doug Reed
Jaime Renner
Jonathan Strain

ADMINISTRATION
Mrs. Cynthia Stocker, Superintendent
Mrs. Beth Lamb, Business Administrator
Mr. Jonathan Kilian, 7-12 Principal
Mrs. Julie Suber, K-6 Principal Intern
Mr. Corey Graves, Athletic Director

May 17, 2019

Rebecca Wilcox, Chief examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, NY 13202-1428

Dear Ms. Wilcox,

The Stockbridge Valley School District has reviewed the draft Information Technology audit completed by your office and transmitted to us via email on April 24, 2019. This letter will comprise the district's Written Audit Response.

The district appreciates the opportunity that this audit provided to examine and better understand our Information Technology practices and procedures, as well as the opportunity to strengthen our technology security.

Upon review of this draft audit, the district is in agreement with the report and findings. We are pleased to report that the district has already taken steps to implement many of your recommendations. The time line for completing all recommendation is summer of 2019. Specific training on changes made to practices and procedures will be communicated to all staff and faculty during Superintendent Conference days in September.

On behalf of the Board of Education and District Administration, I would like to thank the Office of the State Comptroller for the learning experience that this audit offered and for the courtesies and professionalism during this review.

Sincerely,

Cynthia M. Stocker

Cynthia M. Stocker
Superintendent of Schools
Stockbridge Valley CSD

P.O. Box 732 • 6011 Williams Road, Munnsville, NY 13409-0732 • Phone: 315.495.4400 • Fax: 315.495.1901 • www.stockbridgevalley.org

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 interviewed District officials and employees and reviewed the District's IT policies to gain an understanding of its IT environment, internal controls and security awareness training.
- We selected to review 10 computers assigned to 10 employees: the high school principal, elementary school principal, technology coordinator, BOCES network technician, school nurse and five employees in the Business office. We chose these individuals because their duties and computer access permissions involved using and transmitting sensitive electronic data.[5]
- We reviewed the Internet browsing histories on our sample of 10 computers to assess whether there was any inappropriate computer usage.
- We ran computerized audit scripts on our sample of 10 computers to determine whether they contained any unwanted or malicious software.
- We reviewed user account permissions and determined whether they were appropriate based on job functions and needed 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 and administrator accounts and compared them to current employee lists 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 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 Financial, student and health records

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