REPORT OF EXAMINATION | 2019M-27

Charlotte Valley Central School District

Information Technology

SEPTEMBER 2019

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

Contents

Report Highlights

Charlotte Valley Central School District

Audit Objective

Determine whether the Board and District officials ensured District information technology (IT) assets and computerized data were safeguarded.

Key Findings

- The Board and District officials did not monitor computer use policies or adopt adequate IT security policies.
- District officials did not develop procedures for managing, limiting and monitoring user accounts and permissions and securing personal, private and sensitive information (PPSI).
- District officials did not provide IT security awareness training for District employees.

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

Key Recommendations

- Adopt and monitor comprehensive IT security policies.
- Develop comprehensive procedures for managing, limiting and monitoring user accounts and permissions and securing PPSI.
- Provide periodic IT security awareness training to personnel who use IT resources.

District officials generally agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

Background

The Charlotte Valley Central School District (District) serves seven towns in Delaware, Otsego and Schoharie counties.

The District is governed by a five-member Board of Education (Board) that is responsible for the general management and control of the District's financial and education affairs. The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible for the District's administration.

The District contracted with Otsego Northern Catskill Board of Cooperative Educational Services (ONC BOCES) to provide IT services, including an IT coordinator. The IT coordinator was the District's network administrator and was responsible for the overall management of the District's IT infrastructure.

Quick Facts	
Student Enrollment	390
Employees	120
# of Desktop, Laptop and Tablet Computers	538
Server Computers	2

Audit Period

July 1, 2017 – December 6, 2018

We extended our audit period to August 10, 2010 to review employee Internet usage.

Information Technology

The District relied on its IT assets for Internet access, email and for maintaining confidential and sensitive financial, personnel and student records. District officials recently made a significant investment in IT during our audit period that resulted in the assignment of new desktops, laptops and tablets to almost all students and employees.

The District's contract with ONC BOCES includes Broome-Tioga (BT) BOCES regional network services, which includes hosting the majority of the District's confidential and sensitive records. BT BOCES maintains the District's firewall and intrusion detection system.[1]

How Should District Officials Safeguard IT Assets and Computerized Data?

A school district should have acceptable computer use policies (AUPs) 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. In addition, officials should require employees to sign acknowledgement forms to indicate they have received the AUPs to ensure employees are aware of and understand what is expected of them.

Monitoring compliance with AUPs 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 personal, private and sensitive information (PPSI)[2] 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 AUPs allowed the use of District IT assets only for educational purposes.

Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability.

1 A firewall is a software application or hardware device that filters traffic between a trusted network and an untrusted network, such as the Internet. An intrusion detection system (IDS) is a software application or hardware device installed on a network that detects and reports intrusion attempts. A firewall can block a suspicious connection while an IDS cannot.

2 PPSI is any information to which unauthorized access, disclosure, modification or 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.

District officials also should establish IT security policies for all IT assets and information including data classification; the use of and access to PPSI; password security; wireless security; user accounts and permissions; remote access; online banking and the sanitization and disposal of IT equipment. Officials should periodically review these policies, update them as needed and stipulate who is responsible for monitoring policy compliance. In addition, officials should monitor and analyze computer and Internet use for signs of possible violations or imminent threats of violations of these policies.

District Officials Did Not Enforce the Acceptable Computer Use Policies

District officials did not monitor and enforce the AUPs. Although the policies require all users to sign an agreement of the computer use terms, officials enforced this directive for students but not employees. District officials told us they were unaware of this requirement for employees.

We reviewed the Internet browsing histories for 18 user accounts on seven computers and six tablets[3] and found noneducational Internet use for three network accounts. This included online shopping and banking, personal email access, social media use and browsing travel, health, fitness, news and other entertainment websites.

The District's web filtering software is designed to block users from accessing unapproved websites. However, the IT coordinator did not monitor employee Internet use for inappropriate activity that was not automatically blocked by the software, unless an issue was reported to him, because he 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, District computers had an increased risk of exposure to damage, and PPSI contained on the computers had a higher risk of breach, loss and/or misuse.

The Board Did Not Adopt Other Necessary IT Security Policies

The Board did not adopt IT security policies for data classification or the use of and access to PPSI. While the District's breach notification policy and access to electronic communications policy discussed some aspects of maintaining PPSI, the District did not have a policy that addressed collecting, storing and transmitting PPSI or provided procedures for monitoring policy compliance.

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

The Board also did not adopt policies for password security, wireless security, user accounts and permissions, remote access, online banking or the sanitization and disposal of electronic media. Although the District had an asset disposal policy, it was not updated to address IT assets and security risks, including sanitization of devices before disposal. In addition, the AUPs did not address connecting personal mobile and storage devices to the District's network.

District officials told us the IT policies were developed by the previous administration and that they were working on updating all policies. Without adequate IT security policies, officials could not ensure employees were aware of or understood what was expected of them in maintaining the security of District IT assets. As a result, the District had a greater risk that its IT system could have been compromised by attackers or that employees could have inadvertently compromised security measures.

Why Should the District Manage User Accounts and Permissions?

Network accounts enable the system to recognize specific users and grant authorized permissions to users. However, network accounts can be used as potential entry points for attackers because they could be used to inappropriately access and view PPSI. A district should have written procedures for granting, changing and revoking user permissions to the network.

In addition, to minimize the risk of unauthorized access, district officials should regularly review enabled network 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.

Officials are responsible for restricting network account user permissions to only those resources and data that are necessary for employees to perform their job functions. This helps ensure that PPSI is protected from unauthorized access and modifications.

Officials Did Not Adequately Manage User Accounts and Permissions

District officials did not develop procedures for managing, limiting and monitoring user accounts and permissions and securing PPSI. We reviewed the District's 142 employee and generic network accounts[4] and found the following questionable or unneeded accounts:

- 34 accounts (24 percent) had not been used in at least one year. Therefore, we question whether these accounts were needed. These accounts were for a Board member, BOCES employees, substitute teachers, teachers' aides, bus drivers, food service employees and building maintenance employee. The accounts were provided to these individuals for functions such as checking their emails or to participate in online training programs, but were not used routinely.
- 18 accounts (13 percent) did not match the list of current employees, had not been used in at least one year and were unneeded accounts. Eleven were assigned to former substitute teachers, two were for former summer school teachers, one was for a retired employee, one was for a former BOCES employee who previously worked at the District, one was for a prospective District employee and had never been used, one had a misspelled username[5] and one was for the District's attorney that had never been used since it was created in 2009.
- Seven accounts (5 percent) were not assigned to specific individuals, had not been used in at least one year and were unneeded accounts. Four were associated with the setup of server computers, had not been used for more than seven years and were no longer needed. The IT Coordinator disabled these accounts while we were onsite. Another account was a Board account that was available for use by any Board member, but had never been used. Therefore, it was an unneeded account. Additionally, two other accounts, a test account and a classroom account, had not been used in more than a year and were no longer needed.

In addition, we found that three network accounts of three employees had access to staff evaluations that contained PPSI. However, the employees did not need these user permissions to perform their job duties.

---

4 These included network accounts for current and former District employees, current and former BOCES and BT BOCES employees and a prospective District employee who never began employment and 12 generic accounts. Generic accounts are used by certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs. For example, generic accounts can be used for training purposes or as a generic email account, such as a service helpdesk account. Generic accounts that are not related to specific system needs should be routinely evaluated and disabled, if necessary.

5 The employee had an active, correctly spelled user account. The account with a misspelled username was unnecessary because it was not used or removed even after a corrected account was created.

The IT Coordinator told us he periodically reviewed user accounts and permissions, but did not always have sufficient time to thoroughly review them. In addition, the District did not have written procedures for monitoring user accounts and permissions.

Any unneeded network accounts and excessive user permissions should be disabled as soon as they are no longer needed to decrease the risk of unauthorized access and potential entry points for attackers to access PPSI. Furthermore, when the District allows users to use generic accounts, this can prevent officials from tracing suspicious activity and holding responsible users accountable for their actions.

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[6] 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 IT security measures. While the AUPs included some basic guidelines, the District did not have a written policy requiring all users to be trained in proper usage of the IT infrastructure, software and data.

6 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 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?

The Board should:

1. Adopt and periodically review and update comprehensive IT security policies for data classification, the use of and access to PPSI, password security, wireless security, user accounts and permissions, remote access, online banking, the sanitization and disposal of electronic media and IT security awareness training.

2. Update the AUPs to address connecting personal mobile and storage devices to the District's network.

District officials should:

3. Develop procedures for monitoring Internet usage and enforcing the AUPs.

4. Develop comprehensive procedures for managing, limiting and monitoring user accounts and permissions and securing PPSI.

5. Provide periodic IT security awareness training that reflects current risks identified by the IT cybersecurity community to personnel who use IT resources.

District officials should ensure the IT coordinator:

6. Routinely monitors employee Internet use for inappropriate activity that is not automatically blocked by the web filtering software.

7. Thoroughly reviews user accounts and permissions on a routine basis and disables any unneeded network accounts and excessive user permissions as soon as they are no longer needed.

Appendix A: Response From District Officials

Charlotte Valley Central School

"Empowering Students Today to Conquer the Challenges of Tomorrow"

Mr. James Harter, Superintendent

Mr. Mitchell Rapp, Principal

15611 State Hwy 23; Davenport NY, 13750

Phone (607)278-5511 Fax (607)278-5900

August 28, 2019

This letter is an acknowledgement that the New Your State Comptroller's office conducted an extensive IT Audit of Charlotte Valley's IT hardware, software and operating systems including but not limited to internet usage, security and data storage. The audit occurred From July 1st 2017 to December 2018 and covered Internet usage as far back as 2010. ***We generally agree*** with the findings of the Examiner in Chief and their team concerning Board of Education policies that have not been adopted or needed refreshing in an ever changing technological world. We also generally agree that the District needs to continue to be vigilant in security awareness for its employees.

The District found the audit to be helpful in identifying issues that needed to be addressed and/or confirmation that the majority of our IT system generally operates within the boundaries of convention and acceptable IT parameters in the public school environment. The District would concede that our IT staff is that of only 1 person who is employed .8 FTE. The District has already complied with the majority of recommendations in the Audit as suggested by the Examiner in Chief. The district will continue to improve on providing its users, employees and community a fundamentally safe, sound and beneficial educational IT environment.

Sincerely,

James Harter

Superintendent of Schools

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 examined the District's network user accounts and related settings using specialized audit software. We reviewed the network and administrator accounts and compared them to current employee lists to identify inactive and unneeded accounts. We reviewed automated network settings to identify any settings that indicated ineffective IT controls.
- We reviewed the District's IT policies and procedures and interviewed District officials to gain an understanding of the District's IT operations and determine the adequacy of the policies and procedures.
- We used our professional judgment to select 18 user accounts assigned to seven employees, three classrooms, one student and one vendor computer. We selected four of the seven employees for our sample based on job titles that indicated duties likely to involve accessing student, staff and financial PPSI. The 18 user accounts resided on two desktops (seven user accounts), five laptops (five user accounts) and six tablets (six user accounts). The five laptops were assigned to our sample of four employees. We chose to review one desktop and two tablets assigned to classrooms with multiple users, one specialized vendor desktop, two employee tablets that had been assigned to the individuals for a lengthy time period, one random employee tablet and one random student tablet. We reviewed the Internet browsing history for all selected accounts. We used specialized audit software to obtain the Internet browsing history for the 12 user accounts on the seven computers tested (two desktops and five laptops). We manually observed the Internet browsing history for the six user accounts on the six tablets.

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

BINGHAMTON REGIONAL OFFICE – Ann C. Singer, Chief Examiner

State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417

Tel (607) 721-8306 • Fax (607) 721-8313 • Email: Muni-Binghamton@osc.ny.gov

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins counties

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