REPORT OF EXAMINATION | 2019M-147

Binghamton City School District

Information Technology

OCTOBER 2019

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

Contents

Report Highlights

Binghamton City School District

Audit Objective

Determine whether the Board and District officials adequately safeguarded data from abuse or loss.

Key Findings

- Officials do not regularly review network user accounts and disable those that are determined to be unnecessary.
- The Board does not have an adequate contract and separate service level agreement (SLA) for information technology (IT) services provided by the Broome Tioga Board of Cooperative Educational Services' South Central Regional Information Center (SCRIC).
- Officials do not provide periodic IT security awareness training to staff.

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

Key Recommendations

- Regularly review user accounts and disable those that are unnecessary.
- Ensure there is an adequate contract and separate SLA with SCRIC for IT services provided.
- Provide periodic IT security awareness training to personnel who use IT resources.

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

Background

The Binghamton City School District (District) serves the City of Binghamton and the Town of Fenton in Broome County.

The District is governed by a seven-member Board of Education (Board) responsible for the general management and control of the District's financial and education affairs. The Superintendent of Schools (Superintendent) is the chief executive officer responsible for the District's administration. The District contracts with SCRIC to provide IT services, including network administration and the overall management of the District's IT infrastructure.

Quick Facts	
Network User accounts	6,501
Number of desktops, laptops and devices	8,362
Managed IT Service Cost	$1.2 million

Audit Period

July 1, 2017 – May 31, 2019

Information Technology

Why Should a District Disable Unnecessary User Accounts?

Network user accounts enable the system to recognize specific users, grant authorized access rights and provide accountability by affiliating user accounts with specific users. User accounts are potential entry points for attackers because they could be used to access data and view personal, private and sensitive information (PPSI).[1] Officials are responsible for disabling user access to applications, resources and data that are no longer necessary for day-to-day learning, duties and responsibilities to provide reasonable assurance that computer resources are protected from unauthorized viewing, use or modifications. A district should develop procedures for disabling unnecessary user accounts. This includes, but is not limited to having officials regularly reviewing enabled network accounts to ensure they are still needed and disabling unnecessary accounts as soon as there is no longer a need for them.

Officials Did Not Have a Procedure to Disable Unnecessary User Accounts

District and SCRIC staff manage and maintain the District's network access and add, remove and modify user access from the network. We examined 1,510 enabled network user accounts[2] and found 160 accounts were not easily an identifiable match to an existing, active District employee. These accounts were for community members, SCRIC staff or former staff members. Fifty-four of the accounts had not been used in the last 6 months. We did note that none of these accounts were part of a group with administrative access. Typically, administrative access provides users with the ability to do far more with data than just read or view the information. Unnecessary accounts or a user with inappropriate administrative access should be disabled or removed as soon as they are no longer needed to decrease the risk of unauthorized access and potential entry points for attackers to copy, manipulate or delete PPSI.

Officials told us they have not performed a recent review of user accounts to ensure only authorized users have network access. Officials also said they are in the process of developing a more streamlined process, in conjunction with SCRIC, for adding, deleting and modifying user access. The failure to ensure unnecessary user accounts are disabled increases the risk of unauthorized viewing, use or modification of computer information and resources.

---

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 There are 6,501 user accounts with access to the District network. We did not review the settings for students (4,991 accounts) because their access is limited to their personal folders.

Why Should Officials Have an IT Contract and a Separate Service Level Agreement?

A board should have a written contract or agreement with its IT provider that indicates the contract period, services to be provided and basis of compensation for those services. In addition, to protect the district and avoid potential misunderstandings, officials should have a separate written SLA between the district and its IT consultant that identifies the district's needs and expectations and specifies the level of service to be provided.

An SLA is different from a traditional written contract because it establishes comprehensive, measureable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. It provides detailed explanations of the services to be performed by identifying the parties to the contract and defining terminology; term or duration of the agreement; scope and/or subject limitations; service level objectives; performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval processes; and scope of services to be provided.

The District Did Not Have an Adequate IT Contract and Service Level Agreement

The District paid SCRIC approximately $1.2 million in 2018-19 to provide managed IT services. The services are provided as part of the cooperative services agreement with SCRIC for IT services. In addition, the SCRIC provided us with a document called an SCRIC Managed IT Support Matrix (document) that lists 67 services relating to the managed IT services SCRIC provides. The document includes brief descriptions of the services and which party has primary and secondary responsibility for the services but does not include a schedule of reports or other deliverables that will help ensure the District has an understanding of all services to be provided and the roles and responsibilities of the parties. As a result, the document is not as detailed as an SLA should be. For example, the document indicates that SCRIC has the primary responsibility to "maintain a comprehensive technology inventory," but there is no further language to indicate how often the inventory will be updated or when a complete inventory would be available to District officials.

During the course of our audit work, we were provided with IT inventory lists in January and April 2019 which differed by approximately 890 devices. We also found 124 devices that were disposed of in August 2018 that were still listed on the January 2019 inventory as in service, but were not listed on the April 2019 inventory.

Without an adequate contract and separate SLA for IT services, District officials do not have a documented understanding of the services expected to be provided by SCRIC. As a result, District officials have no way to ensure that SCRIC is providing the agreed upon IT services and procedures that protect assets and data from abuse or loss.

Why Should the Board Adopt a Detailed Disaster Recovery Plan?

A strong system of information security controls includes a disaster recovery plan, which describes how officials will deal with potential disasters – that is, any sudden, unplanned catastrophic event such as a fire, flood, computer virus, vandalism or inadvertent employee action that compromises the integrity of computer systems and their associated data. To safeguard data from potential abuse or loss, it is important that the plan be detailed, tested periodically and updated to ensure officials understand their roles and responsibilities in a disaster situation and address any changes in security requirements.

The Disaster Recovery Plan Lacks Necessary Information to Protect Assets and Data

Although the SCRIC provided a disaster recovery plan for the District, it is incomplete. The plan is clearly a template and lacks information. For example, the plan describes annual testing and debriefings conducted by SCRIC with the Executive Management Team (EMT) following the plan's testing. However, it did not specify who the internal contacts would be or define who was on the EMT. District officials told us they were not aware of any testing and had not had any debriefings. As a result, District officials have no assurance that they would be able to protect data against loss or destruction and restore critical IT systems, applications or data timely in the event of a disaster.

Why Should Officials Provide IT Security Awareness Training?

Officials should ensure personnel who use IT resources are aware of security risks and trained in practices that reduce internal and external threats to IT systems and safeguard data from potential abuse or loss. While IT policies tell computer users what to do, periodic IT security awareness training helps them understand their roles and responsibilities and provides them with the skills to perform them. Such training should center on:

- Emerging trends in information theft and other social engineering[3] reminders.
- Limiting the type of PPSI collected, accessed or displayed to that which is essential for the function being performed.

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

- Malicious software, virus protection and the dangers of downloading files and programs from the Internet.
- Password controls.
- The restriction of physical access to IT systems and resources and how to protect them from intentional or unintentional harm, loss or compromise.

Employees Were Not Provided IT Security Awareness Training

Officials did not provide periodic IT security awareness training to staff to help ensure they understood IT security measures to safeguard data from potential abuse or loss. While the District's IT policies include some basic guidelines, the District does not have a written policy requiring all users to be trained in proper usage of the IT infrastructure, software and data. As a result, the District's IT assets and data are more vulnerable to loss and misuse, and employees may not be prepared to recognize and appropriately respond to suspicious system activity.

What Do We Recommend?

District officials should:

1. Develop comprehensive procedures for regularly reviewing user accounts and disabling those that are unnecessary.
2. Provide periodic IT security awareness training to personnel who use IT resources, including the importance of protecting PPSI and restricting physical access to systems and resources.

The Board should:

3. Ensure there is an IT contract and separate SLA with SCRIC for IT services along with a schedule of reports or other deliverables that will help ensure the District has an understanding of all services to be provided and the roles and responsibilities of the parties.
4. Adopt a more comprehensive disaster recovery plan that defines who should be involved in the periodic testing and updating of the plan.

Appendix A: Response From District Officials

Binghamton City School District
Christopher Columbus School
164 Hawley Street
PO Box 2126
Binghamton, NY 13902-2126
(607) 762-8100
Fax: (607) 762-8112

October 11, 2019

Ann C. Singer, Chief Examiner
Statewide Audit
State Office Building, Suite 1702
44 Hawley Street
Binghamton, NY 13901-4417

Dear Ms. Singer:

The Binghamton City School District is in receipt of the Draft Audit Report based on the audit of the district's Information Technology as enacted for the period July 1, 2017 through May 31, 2019. Please consider this letter as the response to the audit, as pursuant to General Municipal and NYS Education Law.

On behalf of the Board of Education and administration, we would first like to thank the local staff of the Comptroller's Office for their professionalism while conducting the audit. The auditor was courteous throughout the process and actively listened to respondents as he engaged with district faculty and staff.

The district is also thankful for the thoroughness of the auditor's action throughout the audit process, which resulted in a minimal number of findings in the approaches used to safeguard data from abuse or loss. The district works directly with managed IT services provided by the Broome-Tioga BOCES to ensure safeguards are put into place. As a result, the material findings cited in the audit were the failure to have an adequate regular review of network user accounts, the lack of regular enhanced training for all faculty and staff on security measures they can take as users of information technology, and the lack of an adequate contract and service level agreement with Broome Tioga BOCES for managed IT services so that timelines and deliverables are easily discerned.

The district agrees with the material findings of the audit. The District's Corrective Action Plan (CAP) will be submitted once a final report is issued and within the required timeframe.

In closing, I would like to, once again, thank the field staff of the Comptroller's Office for their assistance throughout the review. If you have any questions regarding our response, please feel free to contact me.

Respectfully,

Tonia Thompson, Ed.D.
Superintendent of Schools

Educating, empowering and challenging all students to become productive, global citizens through innovative approaches to learning.

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, our audit procedures included the following:

- We interviewed District officials and SCRIC staff to obtain an understanding of the District's IT operations including the safeguards to protect sensitive data, the existence and testing of a disaster recovery plan and if any employees received IT security awareness training.
- We used computerized audit scripts to analyze and access the District's network information about users (administrative and teacher/student) to determine whether user account and security settings were necessary and appropriate. We reviewed user accounts and compared them to a list of current employees to identify potentially inactive and unnecessary accounts. We also analyzed user accounts and security settings applied to those accounts on the District servers.
- We reviewed contractual documents with the District and SCRIC to determine the scope of IT services, reporting requirements, performance indicators and security procedures.
- We compared two IT inventory lists and disposal records to determine whether the lists had changed and if previously disposed of assets were listed on the inventories.

Our audit also examined the adequacy of certain IT 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 GAGAS (generally accepted government auditing standards). 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 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