REPORT OF EXAMINATION | 2020M-157

Hudson City School District

Information Technology

JANUARY 2022

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

Contents

Report Highlights

Hudson City School District

Audit Objective

Determine whether Hudson City School District (District) officials ensured information technology (IT) systems were adequately secured against unauthorized use, access and loss.

Key Findings

District officials did not adequately secure and protect the District's IT systems against unauthorized use, access and loss. The Board and District officials did not:

- Adopt adequate IT policies or a disaster recovery plan.
- Ensure the acceptable use policy (AUP) was complied with, monitor the use of IT resources or provide IT security awareness training. We found questionable Internet use on four of six computers tested.
- Disable 123 of the 462 enabled network accounts we examined. These 123 user accounts were unneeded and included generic and former employee accounts.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt comprehensive IT policies and a disaster recovery plan, and provide periodic IT security awareness training to all employees who use IT resources.
- Develop written procedures for managing system access.

Background

The District serves the City of Hudson and Towns of Claverack, Ghent, Greenport, Livingston, Stockport and Taghkanic in Columbia County. The District is governed by a Board of Education (Board), which has seven elected members.

The Superintendent is appointed by the Board and is the chief executive officer responsible for day-to-day management, under the Board's direction.

The District contracted with an IT service provider to operate and maintain the District's IT system. The Business Administrator is responsible for overseeing the IT service provider.

Quick Facts	
Network User Accounts[a]	3,292
Computers	778
Total Paid to the IT Service Provider	$142,209
Employees	692
Students	1,816

a) These included 462 employee, 2,786 student and 44 generic accounts.

Audit Period

July 1, 2018 – January 31, 2020

Information Technology

The District's IT system and data are valuable resources. The District relies on its IT assets for a variety of tasks, including Internet access, email, and for maintaining financial, personnel and student records, which contain personal, private and sensitive information (PPSI).[1]

If the IT system is compromised, the results can be catastrophic and require extensive effort and resources to evaluate and repair. While effective controls do not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

District officials hired a CPA firm to conduct an IT audit in May 2019 due to some District concerns. The CPA firm's IT audit report (completed before the former IT service provider began providing IT services) contained findings and recommendations. In spite of being made aware of risks to the IT system, including PPSI of employees and students, District officials did not contract with the former IT service provider to implement all the recommendations. This left the District's IT system at risk.

Before July 1, 2019, the District had an in-house IT Department but contracted with the former IT service provider on July 1, 2019 to maintain the District's network. Subsequent to our audit, officials hired another IT professional and moved the IT function back in-house.

The District's IT service provider's role is to provide oversight and advise District administration on the revision of the District IT plan, evaluate the performance of IT department employees, oversee IT training and support, assist in developing and monitoring the annual technology operations budget, and assist in acquisition of new technology and equipment.

During our audit the former IT service provider was onsite at the District two days a week for a one year contract. In addition, the District contracts with the Questar III Board of Cooperative Educational Services for helpdesk support and other services.

How Should IT Systems Be Safeguarded and Protected?

IT policies such as password, wireless security and mobile and removable device policies describe the tools and procedures to protect PPSI and information systems, define appropriate user behavior and explain the consequences of policy violations. A board must establish policies for all IT assets and information, disseminate the policies to officials and staff and ensure that officials monitor and enforce the policies.

1 PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, customers, third parties or citizens of New York in general.

District officials should develop procedures for storing, classifying, accessing and disposing of PPSI. These procedures should define PPSI, explain the district's reasons for collecting PPSI, and describe specific procedures for the use, access to, storage and disposal of PPSI involved in normal business activities.

The Board Did Not Adopt Adequate IT Policies

District officials did not develop, and the Board did not adopt the following IT policies: password security, wireless security, and mobile and removable device policies. Without properly designed and functioning controls there is a likelihood that significant errors or fraud will occur and remain undetected. A lack of appropriate policies significantly increases the risk that data, hardware, and software systems may be lost or damaged by inappropriate access and use. The former IT service provider told us that the District had not developed these policies.

Additionally, the CPA firm that was conducting an IT audit of the District (completed in May 2019) requested evidence supporting the documentation of policies and procedures for IT, but District officials did not provide any. The firm recommended the District draft and implement approved policies and procedures surrounding IT controls and operations. We found the firm's recommendations were not implemented.

Further, the Board and District officials did not develop written policies to define PPSI, explain the reason for collecting PPSI or written procedures for use, access to, storage and disposal of PPSI involved in normal business activities. Also, officials did not establish a data classification scheme or conduct an inventory of PPSI. Unless officials classify this data and set up appropriate security levels for PPSI, there is an increased risk that PPSI could be exposed to unauthorized users, and efforts to properly notify affected parties in the event of a data breach could be hampered.

While policies alone will not guarantee the safety of IT assets and data, without appropriate policies the District has an increased risk that it could lose important data. Also, without a PPSI inventory, District officials cannot ensure that all PPSI is properly accounted for and protected. The failure to protect PPSI can have significant consequences on the District, such as reputation damage, lawsuits, a disruption in operations or a security breach.

Why Should the Board Adopt a Disaster Recovery Plan?

A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. Disasters may include any sudden, catastrophic event (such as a fire, computer virus or inadvertent employee action) that compromises the availability or integrity of an IT system and data.

To minimize the risk of data loss or suffering a serious interruption of service, district officials should establish a formal written disaster recovery plan. The plan should address the potential for sudden, unplanned catastrophic events that compromise the network and the availability or integrity of district services, including the IT system and data.

Typically, a disaster recovery plan involves an analysis of business processes and continuity needs, specific roles of key individuals and precautions needed to maintain or quickly resume operations. The plan should be periodically tested and updated to ensure officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements. Additionally, such a plan should include data backup procedures.[2] Backup data should be stored at an offsite location and encrypted to ensure integrity and periodically be tested to ensure backups will function as expected.

To minimize the risk of data loss or suffering a serious interruption of service, district officials should establish a formal written disaster recovery plan.

The Board Did Not Adopt a Disaster Recovery Plan

The Board did not develop a disaster recovery plan to describe how officials would respond to potential disasters. Consequently, in the event of a disaster or a phishing or a ransomware attack,[3] officials have no guidance or plan to follow to restore or resume essential operations in a timely manner.

Additionally, in May 2019, the CPA firm that conducted the IT audit found the District did not have a business impact analysis (BIA) to identify and prioritize the systems in use for effective resumption of services. The CPA firm recommended the District perform a full BIA, including all lines of business, locations and departments.

The firm advised that a comprehensive continuity or disaster recovery plan should include procedures to recover those key systems and maintain business operation. We found District officials did not ensure that the CPA firm's recommendations were implemented. This occurred because District officials did not include the implementation of recommendations in the former IT service provider's contract.

... District officials did not ensure that the CPA firm's recommendations were implemented.

The former IT service provider told us that the District is in the process of developing a disaster recovery plan but was not at the stage where it could be provided for review. In addition, the Superintendent told us it was not the District's

2 A backup is a copy of electronic information that is maintained for use if there is a loss or damage to the original.

3 Phishing is sending deceptive email messages in an attempt to gather personal information or infect computer systems with malicious software. Ransomware is a type of malicious software that prevents users from accessing their computer systems or electronic data until a ransom payment is made.

intention to have the former IT service provider address all the findings within a year because the District wanted to hire an in-house IT professional by June 30, 2020 to handle most of the findings and recommendations. According to the Superintendent, the former IT service provider worked two days a week and priorities changed due to COVID-19.

However, without a formal written plan, the District has an increased risk that it could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees.

Further, District officials did not perform network backups during our audit period. In addition, the Board did not develop a backup policy or procedures for performing network backups. As a result, officials would not be able to restore operations following a service disruption.

Without a disaster recovery plan, responsible parties may not be aware of steps they should take, or how to continue doing their jobs to resume business in the event of disaster. Also, by not performing network backups, District officials have no assurance that important data will be available in the event of a loss such as a ransomware attack. As a result, the District has an increased risk that it could lose important data and suffer a serious interruption in operations.

Why Should Officials Properly Manage Network User Accounts and Access?

Network user accounts provide users with access to the resources on a district's network and user computers and should be actively managed to minimize the risk of misuse. If not properly managed, network user accounts could be potential entry points for attackers allowing them to inappropriately access and view PPSI, make changes to the records or deny access to electronic information.

A district should have written procedures for granting, changing and disabling user permissions to the network. To minimize the risk of unauthorized access, district officials should actively manage network user accounts, including their creation, use and dormancy, and regularly review enabled network user accounts to ensure they are still needed. Officials should disable unnecessary accounts as soon as there is no longer a need for them, including user accounts of former employees.

Generic accounts are used by certain network services or applications to run properly. For example, generic accounts can be created and used for classroom instructional purposes or to scan student test scores. Officials should routinely evaluate and disable any generic accounts that are not related to a specific system need.

District Officials Did Not Adequately Manage Network User Accounts

The former IT service provider was responsible for ensuring network user accounts were managed in a timely and satisfactory manner. However, network user accounts and permissions were inadequately managed. District officials did not establish procedures to manage these accounts or maintain a list of authorized network users and their level of access. As a result, we found unneeded network user accounts that had not been disabled and/or monitored.

The CPA firm's audit of the District's IT systems found that network user accounts were not reviewed or audited on a regular basis. The firm recommended that, at least annually, the District should administer regular re-certifications of all users to ensure that user's access level is agreeable to their specific job duties and responsibilities.

We found the CPA firm's recommendation was not implemented, and the District did not respond to the finding because officials did not include implementing all recommendations in the former IT service provider's contract.

When new employees were hired or left District employment, the District Clerk or Human Resources Department would notify the former IT service provider the level of access needed in writing. However, officials did not have a formal process or written procedures in place for adding or disabling network user accounts.

We reviewed all 462 employee network accounts and found 89 enabled network accounts (19 percent) were for former employees. The former IT service provider told us that currently there was no available information to determine who owned which account, and District officials are working on rebuilding a new IT environment where only necessary network accounts would be present. Because these network user accounts were not disabled, they could potentially be used by those individuals or others for malicious purposes.

In addition, during our review of all 44 generic accounts, we found 34 generic accounts that were originally created for various uses and were no longer needed. After we notified the former IT service provider of these unneeded accounts, he told us that this will be corrected as part of the District creating a new IT environment so that only necessary accounts remain. We recommend disabling these unneeded accounts immediately.

Unneeded network user accounts can be potential entry points for attackers and could be used to inappropriately access and view PPSI. In addition, when the District has many network user accounts that must be managed and reviewed, unneeded user accounts may make it more difficult to manage network and computer access.

... [T]he CPA firm's recommendation was not implemented, and the District did not respond to the finding because officials did not include implementing all recommendations in the former IT service provider's contract.

How Should Officials Monitor Compliance with the AUP?

An AUP describes what constitutes appropriate and inappropriate use of IT resources, along with district management's expectations concerning personal use of IT equipment, and user privacy and consequences for violating the AUP.

Monitoring compliance with the AUP 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, the AUP 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 malicious software 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 limit access to sites that comply with a district's AUP.

We found questionable Internet use on four of the six computers tested…

Officials Did Not Monitor for AUP Compliance

The District's comprehensive AUP defines the procedures for computer, Internet, and email use. The policy describes what constitutes appropriate and inappropriate use of IT resources and states that the Internet is to be used exclusively for instructional, research and administrative purposes. We reviewed the web browsing history of six computers used by employees whose job duties routinely involved accessing PPSI.[4] We found questionable Internet use on four of the six computers tested, which included social media use, personal online shopping and banking, entertainment, travel and non-District related activities or subjects. Because District officials did not monitor employee Internet use, they were unaware of this personal and inappropriate computer use.

By allowing personal use of computers, the District has an increased risk that its network and computers will be exposed to attacks and 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

4 Refer to Appendix B for information on our sampling methodology.

Why Should 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 behavior for using the Internet and IT systems and data. In addition, the training should communicate related policies and procedures to all employees.

The training should center on emerging trends such as information theft, social engineering attacks, computer viruses, and other types of malicious software, all of which may result in PPSI compromise or denying access to the IT system and its data.[5] 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 Internet browsing and downloading files and programs from the Internet, requirements related to protecting PPSI and how to respond if an information security breach is detected.

District officials did not provide employees with IT security awareness training…

Officials Did Not Provide IT Security Awareness Training

District officials did not provide employees with IT security awareness training to help ensure they understand IT security measures designed to safeguard data and IT assets. As a result, IT assets and data were more vulnerable to loss and misuse.

The IT audit the CPA firm conducted found that IT security awareness training was not in place for all District employees. The firm recommended that District officials create and implement a training program annually for all employees in which the risks of information technology, and the efforts each employee can put forth to increase security are communicated to staff. We found that District officials did not ensure that the CPA firm's recommendation was implemented.

The former IT service provider's contract stated that he will oversee training and support. The former IT service provider told us that a cybersecurity module was e-mailed to employees. However, we interviewed four District office employees who said they did not receive any IT training.

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, District data and PPSI could be at greater risk for unauthorized access, misuse or loss.

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

What Do We Recommend?

The Board should:

1. Require timely implementation of corrective action in response to the CPA report and this report on IT controls.

2. Adopt comprehensive IT security policies to address passwords, wireless security, and mobile and removable devices and communicate all adopted IT policies to District officials, employees and the IT service provider.[6]

District officials should:

3. Develop a PPSI policy and inventory by classifying all District data and identifying where it is stored in the computer system and who uses it. Also, periodically review and update the inventory.

4. Develop and test a comprehensive disaster recovery plan that identifies key personnel, including data backup procedures and offsite storage, and test the plan to ensure it works as intended.

5. Develop written procedures for managing system access that include periodically reviewing user access and disabling network user accounts when access is no longer needed.

6. Design and implement procedures to monitor the use of IT resources, including personal use, for compliance with the AUP.

7. Provide periodic IT security awareness training to all employees who use IT resources that includes guidance on the importance of appropriate computer use.

6 Refer to our publication *Information Technology Governance*
http://www.osc.state.ny.us/files/local-government/publications/pdf/itgovernance.pdf.

Appendix A: Response From District Officials

Hudson City School District
215 Harry Howard Avenue
Hudson, New York 12534-1606
▶ Home of the Bluehawks ◀
District Office
(518) 828-4360 Ext. 2101
Fax: (518) 697-8315

January 5, 2022

Lisa Reynolds, Chief Examiner
Newburgh Regional Office
33 Airport Center Drive
Suite 103
New Windsor, NY 12553

Dear Ms. Reynolds:

This letter acknowledges receipt of the Draft Report of Examination for the Hudson City School District which includes the results of the extensive Information Technology Audit conducted by the New York State Comptroller's Office during the period of July 1, 2018 to January 31, 2020. Please accept this letter as the District's response to the audit, as pursuant to General Municipal and NYS Education Law.

On behalf of the Board of Education and administration, we would like to first thank the assigned staff for their professionalism while on district premises to conduct the audit. The District is grateful for the opportunity to receive valuable feedback to improve our policies and practices related to information security and privacy measures. This is a critically important area of school life and we appreciate having specific guidance on the improvements that are required.

We agree with the findings documented in the audit and find the facts contained within the report to be accurate and complete for the period of July 1, 2018 to January 31, 2020. We agree with the recommendations provided in the draft report. We prepared our Corrective Action Plan and submitted it June 2021, after it was approved by the Board of Education.

At the time of the Audit, planning was already underway to address many of the identified deficiencies. Therefore, at the writing of this letter, the District has fully complied with the recommendations in the Audit. The District was and still is in the process of transitioning and transforming its IT operations beginning with a change in staffing and related services. Significant resources have been applied to address the equipment, network, and operating deficiencies and the District will continue to improve our infrastructure to provide all users with a secure, stable, scalable, and sustainable IT environment.

In closing, I want to once again thank you for the professionalism of your staff and the opportunity to have clear guidance on what the District needs to specifically address.

Respectfully submitted,

Dr. Maria Lagana Suttmeier
Superintendent of Schools

DESTINATION GRADUATION TO OCCUPATION

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 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 reviewed service level agreements and interviewed officials to understand the roles and responsibilities of the District's IT staff.
- We inquired about a breach notification policy, PPSI policy, disaster recovery plan and backup procedures to determine whether these policies, plans and procedures were adopted and working as intended.
- We interviewed officials and personnel to gain an understanding of the IT environment and internal controls over IT assets.
- We used a specialized audit script to examine the District's domain controller.[7] We then analyzed the report to determine whether all users were currently employed by the District.
- We used our professional judgment to select a sample of six of the 34 computers used by employees. We selected our sample based on those employees who had access to PPSI.[8] We reviewed the web browsing histories on these six computers to determine whether Internet use was in compliance with the District's AUP guidelines.
- We reviewed recommendations made by the CPA firm that conducted an audit of the District's IT to determine whether recommendations were implemented.

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 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.

7 The domain controller is the main server computer in the domain (network) that controls or manages all computers within the domain.

8 These users had access to either key financial applications and/or related PPSI including online banking, payroll, and human resources information.

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.

The Board has the responsibility to initiate corrective action. 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-a(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 next 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. The CAP should be posted to the District's website for public review.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2018-12/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263196&issued=All

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263206&issued=All

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2020-05/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/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263211&issued=All

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

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/local-government

Local Government and School Accountability Help Line: (866) 321-8503

NEWBURGH REGIONAL OFFICE – Lisa A. Reynolds, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Sullivan, Rockland, Ulster, Westchester counties

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