Patchogue-Medford School District

Review of
Information Technology Environment
And
nVision Access Permissions

December 2017

December 2017

The Board of Education
Patchogue-Medford Union Free School District
241 South Ocean Avenue
Patchogue, NY 11772

Board of Education:

We have been retained to function as the internal auditor for the Patchogue-Medford Union Free School District (hereinafter, "the District"). Our responsibility is to assess the internal control system in place within the District, and to make recommendations to improve upon identified control weaknesses or deficiencies, if any. In doing so, we hope to provide assurance to the District's Board, management, and residents, that the fiscal operations of the District are being handled appropriately and effectively.

BACKGROUND

As part of the detailed risk assessment performed during the 2014-2015 school year, we recommended performing a review of the information technology environment. The District's prior internal auditors performed a test of this area and issued the results of their review and recommendations in November 2013. The District has implemented or is in the process of addressing the recommendations. Since there have been significant changes in technology, the Audit Committee requested that internal audit reassess the internal controls within the information technology environment. In addition, as the District recently converted the financial software application from Finance Manger to nVision, we were requested to assess the access permissions specifically to this application.

INFORMATION TECHNOLOGY ENVIRONMENT

Our objective was to assess the District's internal controls to determine if computer equipment, software, and data are adequately safeguarded. The IT functions in the District are performed under the direct supervision of the Director of Technology. The IT Department is responsible for daily systems support, network access support, as well as a backing up and restoring data. To perform our review of the information technology environment, we discussed the roles and responsibilities of District staff and assessed the controls that are in place that relate to information technology, focusing on policies, access controls, and continuity of business operations. In addition, we utilized the Information Technology (IT) Systems Self-Assessment Questionnaire from the Information Technology Guidance produced by the New York State Comptroller's Office, as well as an internally created IT Questionnaire.

The results of our review are documented in Section I of this report.

ACCESS PERMISSIONS

Access permission controls are intended to provide reasonable assurance that computer resources are protected from unauthorized use and modifications. We previously performed a review of access permissions and issued a report to the Board dated June 2015 of the results of review and any recommendations. The District has since implemented any recommendations. Since the District recently upgraded its financial

application software Finance Manager to nVision, we gained an understanding of how access is granted and then verified that the access permissions within this application are properly restricted, that proper segregation of duties exists, and that access is limited based on the user's job descriptions and responsibilities. The results of this review are documented in Section II of this report.

SECTION I. INFORMATION TECHNOLOGY ENVIRONMENT

A. INFORMATION TECHNOLOGY POLICIES AND PROCEDURES

The Information Technology (IT) department has prepared a comprehensive Technology Plan that details the District's current computing environment, and the recommendations needed for handling future growth and to support the entire District's educational initiatives. The District evaluates the action items within the Plan on a regular basis to ensure emerging technology is being considered. The District completed the Technology Plan Survey, and they have implemented, and will continue to implement technology with the funds from the Smart Schools Bond act.

The District also has a Technology Committee for the purpose of advising the Board and making recommendations regarding the purchase and use of technology in the District. The committee recently agreed that the primary focus of the District's technology initiatives should incorporate upgrading the District's firewall and increasing the District-wide high-speed wireless connectivity consistent with the District's Instructional Technology Plan.

Good governance and accountability require the District's Board to adopt policies and procedures to safeguard District data against unauthorized access, misuse, or abuse. The State Comptroller's Office issued an Information Technology Governance Guide dated March 2012 that includes several recommended policies that school district's should adopt.

Auditor's Assessment: The District's website has several key IT policies including a Computer Network and Internet Use Policy that specifies protocols for proper utilization of the District's technology resources and is addressed to all staff and students. We noted that the Board adopted policies that include password management, access rights, remote access, breach notification, user accounts, and data backups. These policies are periodically reviewed and revised as needed to reflect changes in technology or the District's IT environment. Based on our review of the policies in place, the District has taken appropriate measures to implement policies and procedures to reduce the risk that data, hardware, and software systems may be lost or damaged by inappropriate access and use.

We did note, however, that the District does not have a computer policy for the protection of personal, private and sensitive information (PPSI). This policy, which is recommended by the State Comptroller's office, should: define personal, private, and sensitive information (PPSI); explain the entity's reasons for collecting PPSI; and describe specific procedures for the use, access to, storage, and disposal of PPSI involved in normal business activities.

In addition, we noted that District is in the process of adopting a data destruction policy which would address the process for identifying computer equipment that is deemed to be obsolete, and the process for ensuing sensitive information is properly deleted to minimize the risk of unauthorized release of confidential data and/or information.

Recommendation #1: We recommend that the District adopt a policy regarding the protection of personal, private, and sensitive information (PPSI). In addition, we recommend that the District finalize and adopt the policy on data destruction. The implementation of these policies will help to ensure the District's technology environment is adequately safeguarded.

Management's Response: *The data destruction policy has been board approved. The Administrator of Technology will develop a policy regarding PPSI and review with the Assistant Superintendent for Business. Once reviewed, the Assistant Superintendent for Business will recommend to Board for adoption.*

B. INTERNAL/EXTERNAL SECURITY THREATS

Networks are often connected to the Internet, and therefore, connected to users all over the world, as well as networks which may not be known. These connections are needed in order to obtain information; however, such accessibility increases the risk of access and attack from unauthorized individuals. Good computing practice is to implement firewalls, which consist of hardware and/or software that enforce boundaries between computer systems and the Internet. Firewalls control network traffic flows, using rule sets which specify which services will pass through the firewall and which services are kept out. Firewalls can also act as effective tracking tools and can perform important logging and auditing functions. As such, the school district network administrator should log and periodically review firewall activities/events.

Auditor's Assessment: The District has installed network monitoring software that collects various statistics from each of the networks, and also retains the data providing the historical usage performance. This enables the District to receive warnings of potential threats, and alerts if there are variances in performance, such as outages or significant spikes in usage. The software provides information as to who is using the network and what kind of use is occurring (e.g. downloading or possible hacking) thereby helping the District take proactive measures to ensure access to the network will not be compromised. Based on the mechanisms and procedures implemented, the District has taken steps to reduce the risk of unauthorized access due to internal and external threats. **No exceptions noted**.

C. NETWORK ACCESS

The first step in implementing adequate access controls is determining what level and type of protection is appropriate for various resources (e.g., data) and who needs access to these resources. The objectives of limiting access are to ensure that: outsiders (e.g., attackers) cannot gain unauthorized access to systems or data, access to sensitive resources such as operating systems and security software programs are limited to very few individuals who have a valid business need for such access, and employees and

contractors are restricted from performing incompatible functions or functions beyond their responsibilities.

Auditor's Assessment: Access to the District's network (for both adding and changing user access) requires the completion of new account user form or change of access request form, that is initiated by Human Resources, and then sent to various District personnel to be reviewed and implemented. We noted where internal controls over network passwords needs to be strengthened. As a result, this increases the risk of unauthorized access. Due to the sensitive nature of this information, specific vulnerabilities are not discussed in this report but have been communicated to District officials so they can take corrective action.

Recommendation #2: We were informed that the District is aware of the issue and is in the process of implementing technology to improve network password controls. We recommend that the District continue to address the need to strengthen the network access security controls.

***Management's Response*:** *The District acknowledges that network password controls can be improved and has developed a network access security controls policy. Once reviewed by the Assistant Superintendent for Business it will be recommended to the Board for approval*

D. WIRELESS ACCESS

Wireless networks (Wi-Fi) are exposed to many of the same types of threats and vulnerabilities as wired networks, including viruses, malware, unauthorized access, and loss of data. However, they are considered inherently less secure than wired networks because their information-bearing signals are broadcast or transmitted into the air. These traveling signals can, potentially, be intercepted and exploited by individuals with malicious intent. Since wireless networks are used as extensions of wired networks, the security problems of a wireless segment can affect an entire network. A wireless environment, therefore, requires certain additional security precautions.

Auditor's Assessment: We noted that the District has implemented protocols that require users to log on and go through the District's website to gain access to the Internet. This includes access from a District-owned device as well as any personal device that uses the District's Wi-Fi. The District monitors internet activity and is able to limit streaming so that accessibility is not degraded. **No exceptions noted**.

E. REMOTE ACCESS

Remote access is defined as "the ability of an organization's users to access its nonpublic computing resources from locations other than the organization's facilities" (NIST SP 800 - 114). Many school districts permit users and/or vendors to access district resources remotely for a variety of reasons. It is therefore critical that such access be restricted and secured.

Auditor's Assessment: The District permits certain vendors to remotely access the District's network and select applications using a secure access through Remote Desktop VMware. The District has anti-virus security software, internet filters, and a firewall implemented to prevent viruses and unauthorized use. In addition, the District has a policy regarding the standards for connecting to the District's network

from any external host. Based on our review, the District has implemented procedures to minimize the potential exposure to unauthorized remote access. **No exceptions noted**.

F. WEB FILTERING

Many school district employees require access to the internet to perform job functions. In addition, teachers and students both utilize the internet as part of the educational process. School districts often use a web filter to keep students off restricted sites, ensure staff are accessing sites that are needed to conduct legitimate business activities, and ensure that the school's bandwidth is used appropriately. One of the challenges schools face is adequately restricting access to web sites while not impeding business functions or educational activities. With the increase in cybercriminal activity, it is important that access to certain web sites is properly restricted to reduce the threat of unauthorized access.

Auditor's Assessment: The Children's Internet Protection Act (CIPA) specifically requires schools and libraries to block or filter internet access to pictures and material that are "obscene, child pornography, or harmful to minors" on computers that are used by students under 17 years of age. The District's acceptable use policy provides employees and students with guidelines for IT asset use and security. Specifically, the policy prohibits the use of District computers for non-educational or illegal purposes.

We utilized a student user account and a staff user account provided by the District to assess what websites were blocked by the web filter. We noted that the application used to filter internet access is outdated and does not permit the District to be fully compliant with CIPA's access restrictions. We understand that the District will be upgrading the firewall which will permit the District to implement software with better filtering capabilities to restrict access to websites.

Recommendation #3: To ensure internet access by staff and students is in compliance with the District's acceptable use policy as well as CIPA, we recommend that the District implement software protocols to ensure that access to the internet is appropriately restricted.

Management's Response: *The District recognizes the urgency of addressing this issue and is taking proactive measures to replace the antiquated firewall as soon as possible, but no later than September 2018***.**

G. CYBERSECURITY TRAINING

With the increase in cybercriminal activity, it is critical that school districts ensure that its users are educated in proper Internet use to reduce the risk of security breaches. Providing cybersecurity education to staff and students has become a top priority given the number of breaches that have recently occurred. Cybersecurity education includes understanding what information should be protected, and methods that should be incorporated into everyday access to ensure school district data is protected from unauthorized use, modification, or exploitation.

Auditor's Assessment: The District has adopted an acceptable use policy for the use of District-owned computers, email and internet access. However, users (i.e. staff,

teachers, and students) are not provided with formal education on cybersecurity protocols. Such training can include implementing publications on the District's website, providing email notifications of issues and potential threats, providing classes for staff and students on proper internet access and searching , and providing education to both students and staff on internet use and safety protocols.

Recommendation #4: We recommend that the District ensure all users, including teachers, staff and students, are provided with education and training on internet usage to reduce the risk of unauthorized access and/or viruses.

Management's Response**:** *The District will require all employees with computer access to review a mandated electronic video relating to internet usages and protocols. Technology staff will reinforce protocols with teachers responsible for technology instruction to students.*

H. DATA BACKUP & RECOVERY

A backup is a copy of electronic information that is maintained for use if there is loss or damage to the original. There are four important components to any back-up process:

- Backing up data at regular intervals;
- Verifying the data has been backed up;
- Storing the backup media in a secure, (preferably off-site) location ; and
- Verifying the ability to restore the backup data.

Recovery is the process by which an entity can resume business after a disruptive event. The event might be something large, such as a disaster from a major flood, or something small, such as malfunctioning software caused by a computer virus. Recovery procedures need to encompass how employees will communicate, where they will go if a large disruption, and how they will continue to do their jobs. The details can vary greatly depending on the size and scope of the entity and its computerized operations.

Auditor's Assessment: The District systems are backed up internally using VEEAM and sent to a site at another location within District. All services and network switches have Uninterruptible Power Supply (UPS) units which permit the District to safely shut down systems in the event of an emergency or power failure. The District has restored data that is backed up to ensure the backup process is working correctly. Several of the programs utilized by the District are Web-based (IEP Direct and My Learning Plan). As such, the backup and updates occur remotely by the application service provider. In addition, the District's has prepared a comprehensive Disaster Recovery Plan that is updated annually to incorporate any changes in the technology environment. Based on the backup and recovery procedures in place, the District has implemented adequate measures to reduce the risk of delayed or interrupted computer operations, and prevent the loss of equipment and data. **No exceptions noted.**

I. IT EQUIPMENT INVENTORY

Maintaining detailed, up-to-date inventory records for all computer hardware is essential so that the current technology infrastructure is accurately represented, and so that future technology needs can be determined. The information maintained for each piece of computer equipment should include a description of the item including the make, model, and serial number; the name of the employee to whom the equipment is assigned, if

applicable; the physical location of the asset; and relevant purchase or lease information including the acquisition date.

Auditor's Assessment: The Director of Technology along with the Purchasing Agent are responsible for information technology purchases as well as any technology repairs. The Technology Help Desk Support staff assist in all department purchase orders, equipment is inventoried at the building level by the Computer Aides, and the all purchases must be authorized by the Director of Technology. Equipment is tracked on a spreadsheet, and asset tags and inventory forms are distributed from the Accounting Office to each building to tag any new equipment. Assets greater than $1,500 are tagged with bar codes. We noted that staff that receive a laptop are required to sign an agreement. Currently, students do not receive devices to take home. Furthermore, the District has adopted an Acceptable Use Policy that outlines computer guidelines and protocols. **No exceptions noted**.

SECTION II. REVIEW OF ACCESS PERMISSIONS

We obtained a report of all users' access permissions within nVision as of November 29, 2017. nVision contains several modules for performing various financial and human resources functions including payroll, human resources, accounts payable, and accounting. Access within nVision is role-based meaning that users are assigned to a group, and each group is assigned specific access permissions to the modules. Permission changes are performed by users who are assigned to the User/System Administrator group.

nVision has the ability to produce a log indicating when, where, and who uses the computer system. It can also generate a log of all changes made to the information included in the vendor master files. Because virtually all District accounting records and reports are computer generated, it is important that District officials review audit logs periodically. Without such a review, the District does not have adequate assurance that changes to its financial information are appropriate and authorized.

Auditor's Assessment: Based on the access capabilities listed, we assessed if the permissions granted are those functions needed to be performed within the selected employees' job duties, and that each employee is restricted from performing multiple aspects of a financial transaction that could compromise proper segregation of duties. We noted that users are assigned to groups with access permissions that correlate to their job responsibilities. In addition, we noted that the Assistant Superintendent for Business regularly reviews payroll comparison reports as well as payroll edit logs.

We did note, however, that the District is currently in the process of finalizing the implementation of nVision. As a result, the District has assigned system administrator capabilities to the Accounting Supervisor temporarily to ensure the system is correctly processing financial information. Users with administrative access rights can create, delete and modify user accounts and access rights, and increase the risk of unauthorized changes to be made to the accounting records and financial software security settings.

Recommendation #5: The State Comptroller recommends that "the financial system administrator should not be involved in financial operations", and "if this is not feasible, then system activity should be periodically reviewed, and audit logs should be generated and reviewed on a regular basis." We recommend that access permissions be reviewed at least annually to ensure proper segregation of duties, in particular, the assignment of system administrator capabilities. In addition, financial software audit logs and change reports should be routinely reviewed to monitor user activity and compliance with computer use policies.

Management's Response: *During the process of upgrading the software to the nVision platform, it was not feasible for the Technology Department to manage the changes associated with position mapping, permissions and overall system management. Now that the conversion has been completed, changes to permissions will be authorized by the Assistant Superintendent for Business and changes inputted by the Network and Systems Specialist One. In addition, the Internal Claims Auditor, in connection with the Assistant Superintendent for Business will review system activity on a quarterly basis. Furthermore, financial software and change reports will be reviewed on a monthly basis. Access permissions will be reviewed annually. The District will provide reports to the Board in accordance with the timeframes indicated above. Any concerns will promptly be addressed and reported to the Superintendent and Board of Education.*

We would like to thank the staff at the District for their cooperation and professionalism during our testing.

We understand the fiduciary duty of the Board of Education, as well as the role of the internal auditor in ensuring that the proper control systems are in place and functioning consistently with the Board's policies and procedures.

Should you have any questions regarding anything included in our report, please do not hesitate to contact us at (631) 582-1600.

Sincerely,

Cerini & Associates LLP

Cerini & Associates, LLP
Internal Auditors