DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2020M-37

Town of Patterson

Information Technology

JUNE 2020

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Town of Patterson

Audit Objective

Determine whether Town officials ensured the Town's information technology (IT) systems were adequately secured and protected against unauthorized use, access and loss.

Key Findings

- The Board did not adopt adequate IT policies or a disaster recovery plan
- Town officials did not have a service level agreement (SLA) with the IT consultant.
- Town officials did not provide IT security awareness training to staff.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt comprehensive IT policies and a disaster recovery plan.
- Enter into an SLA with the IT consultant for all services to be provided that sufficiently defines the roles and responsibilities of each party and addresses confidentiality and protection of personal, private and sensitive information (PPSI).
- Provide periodic IT security awareness training to all employees who use IT resources.

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

Background

The Town of Patterson (Town) is located in Putnam County. The Town is governed by an elected five-member Board composed of four Board members and the Town Supervisor (Supervisor). The Board is responsible for managing operations.

The Town contracts with an IT consultant to perform IT-related services. The Supervisor is the network administrator and helps the IT consultant provide general IT support to all departments and employees. The Supervisor, in consultation with the IT consultant also makes recommendations to the Board regarding hardware and software application acquisitions and/or changes. The Town has two independent computer networks that contain all user accounts.

Quick Facts	
Employees	162
Network user accounts	52
Servers	2
Computers	40
Total paid to IT Consultant for the Audit Period	$19,112

Audit Period

January 1, 2018 - November 26, 2019

Information Technology

How Should IT Assets Be Safeguarded and Protected?

The Town relies on its IT assets for Internet access, email and for maintenance of financial, personnel and taxpayer records, much of which contained PPSI.[1] If the IT system is compromised, the results could range from an inconvenience to a catastrophe and could require extensive effort and resources to evaluate and repair. While effective controls will 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.

IT security policies describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. A board should establish security policies for all IT assets and information, disseminate the policies to officials and staff and ensure that officials monitor and enforce the policies.

New York State Technology Law requires municipalities to adopt a breach notification policy or local law that details actions to be taken to notify affected individuals when there is system security breach involving personal information.[2] In addition, IT security policies should address data classification and regulations that ensure officials identify and organize town data to determine what data exists, where it is located and how to protect it.[3]

Because different kinds of information require different levels of protection, the nature of the data has to be evaluated so that appropriate internal controls can be established and monitored. In some instances, laws, regulations or a town's policies predefine the classification of each data type. To minimize the risk of data loss or suffering a serious interruption of services, town officials should establish a formal written disaster recovery plan.

This is particularly important given the current and growing threat of phishing and ransomware attacks.[4] The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, flood, computer virus or inadvertent employee action) that could compromise the network and the availability or integrity of the financial system and any PPSI contained therein.

[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.

[2] New York State Technology Law, section 208

[3] Data classification is the process of assigning data to a category that will help determine the level of internal controls over that data.

[4] 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.

Typically, a disaster recovery plan involves analyzing business processes and continuity needs, assuming that all relevant disasters will occur and identifying roles of key individuals and necessary precautions to take to maintain or quickly resume operations. Additionally, a plan should include data backup procedures, such as ensuring a backup is stored off-site in case the building is destroyed or inaccessible, and periodic backup testing to ensure backups will function as expected.

Because computer viruses, such as ransomware, can be idle for a period of time before attacking an IT system, it is possible for recent backups to also contain viruses. Therefore, it is essential to have well-developed procedures for backing up and storing data. The board should periodically review these policies, update them as needed and stipulate who is responsible for monitoring IT policies.

The Board Did Not Adopt Adequate IT Security Policies

Breach Notification Policy – Town officials have not developed and adopted a breach notification policy or local law because they were unaware of this requirement. As a result, if PPSI is compromised, officials may not be able to fulfill the Town's legal obligation to notify the affected individuals to inform those individuals of the need to monitor credit reports and bank activity.

Use of, Access to and Storage and Disposal of PPSI – Town officials have not adopted a policy that identifies the types of PPSI stored, explains the reason for collecting PPSI or specific procedures for use, access to, storage and disposal of PPSI involved in normal business activities. Furthermore, officials have not established a data classification scheme or conducted an inventory of PPSI. Unless officials classify the data they maintain 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.

Disaster Recovery Plan – The Board did not develop a disaster recovery plan to address potential disasters. Consequently, in the event of a disaster or a phishing or ransomware attack, officials have no guidance or plan to follow to minimize or prevent the loss of equipment or data. Officials have not identified, documented and prioritized essential systems and data, which increases potential losses, business and systems downtime and the potential overall cost.

Town officials told us that they are in the process of developing a disaster recovery plan. Without a formal written plan, the Town could lose important equipment, financial and other data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees.

Backup Policy – The IT consultant regularly backed up data for the Town at an off-site location. However, Town officials did not develop written policies or procedures describing the backup process. Although the Supervisor told us that backups were regularly performed, there was no evidence or documentation that officials attempted to restore a backup to ensure the process was functioning as intended and that data would be available in the event of an emergency. Without a formal written backup procedures, the Town is at increased risk that it could not restore operations quickly and effectively following a service disruption.

While policies alone will not guarantee the safety of IT assets and data, a lack of appropriate policies significantly increases the risk that data, hardware and software may be lost or damaged by unintentional or inappropriate use or access.

How Should Officials Monitor and Enforce the Acceptable Use Policy?

A town should have a written acceptable use policy (AUP) that defines the procedures for computer, Internet and email use and describes what constitutes appropriate and inappropriate use of IT resources, 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, 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 malicious software that may compromise data confidentiality, integrity or availability. Town officials can reduce the risks to PPSI and IT assets by routinely monitoring Internet use and developing and implementing procedures to ensure employee compliance with the AUP. In addition, such activity may interfere with an employee's job performance or productivity, lead to inadvertent information disclosure or, when online banking is involved, theft of Town funds.

Officials Did Not Enforce the AUP

The Town has a comprehensive AUP that defines the procedures for computer, Internet and email use. The policy describes what constitutes appropriate and inappropriate use of IT resources and the Board's expectations concerning personal use of IT equipment and user privacy. Further, the policy prohibits the use of Town computer system for personal purposes.

In addition, Town officials required all employees to sign acknowledgement forms indicating they read and understood the policy. We reviewed the forms of five employees and found that all of them acknowledged the policy.[5] However, officials did not design or implement procedures to monitor compliance with the policy or determine the amount of time Town computers were used by employees for personal purposes.

We reviewed the web browsing history of five computers and found questionable Internet use on three computers.[6] This included social media use, personal shopping, online banking, entertainment websites (including streaming) and web searches for non-Town related subjects. The employees using these computers performed job duties that routinely involved accessing PPSI. Because Town officials did not monitor employee Internet use, they were unaware of this personal and inappropriate computer use.

Because Internet browsing increases the likelihood of the Town's computer system being exposed to malicious software that may compromise PPSI, Town computers and any PPSI contained has a higher risk of exposure to damage and PPSI breach, loss or misuse.

Why Should the Officials Properly Manage User Accounts?

User accounts provide access to a town's network and should be actively managed to minimize the risk of misuse. If not properly managed, user accounts could be potential entry points for attackers because they could be used to inappropriately access and view PPSI on the network. A town should have written procedures for granting, changing and disabling user permissions to the network and the financial software application.

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

Officials Did Not Adequately Manage User Accounts

Although the IT consultant was responsible for ensuring user accounts for the IT system were managed in a timely and satisfactory manner, Town officials did not develop comprehensive written policies and procedures for managing system

[5] Refer to Appendix B for information on our sampling methodology.

[6] Ibid.

access and did not adequately manage user accounts for its network. As a result, we found unnecessary user accounts that were not disabled.

We reviewed all of the Town's 52 network accounts and found that seven accounts belonged to former employees who are no longer employed. One of these accounts has not been used since January 2016 and three of the accounts were for former employees who never logged onto the network. The Supervisor disabled these accounts after we notified him of the accounts for employees who are no longer employed.

Without formal procedures for regularly reviewing enabled user accounts, the Town had a greater risk that the unneeded accounts could be compromised or used for malicious purposes. Any unneeded network accounts 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.

Why Should the Town Have an SLA with the IT Consultant?

To protect the Town's IT assets and avoid potential misunderstandings, officials should have a written SLA with its IT consultant that clearly states the Town's needs and expectations and specifies the level of service to be provided by the IT consultant. The agreement must include provisions relating to confidentiality and protection of PPSI and specify the level of service to be provided.

An SLA is different from a traditional written contract in that it establishes comprehensive, measurable performance targets so there is a mutual understanding of the nature and required level of services to be provided. It should provide detailed explanations of the services to be performed by identifying the parties to the contract and defining terminology; duration of the agreement; scope and/or subject limitations; service level objectives and performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval process; and pricing, billing and terms of payment. The SLA should be periodically reviewed by knowledgeable IT staff and legal counsel especially if the IT environment or needs significantly change.

Officials Did Not Have an SLA with the IT Consultant

The Town did not have an SLA for IT services. The Board did not negotiate a formal agreement or SLA with its IT consultant to identify the provider's responsibilities and specific services to be provided. Town officials told us that they did not have an SLA because they were unaware of the benefits of having such an agreement. Instead, the Town had an informal agreement with the IT consultant who was called on from time to time when services were needed.

Town officials told us that they have prepared a draft SLA that still needs to be adopted by the Board. However, without a written contract, in the event of any failure in IT controls (such as a breach), by either the Town or the IT consultant, the lack of a specific SLA can contribute to confusion over who is responsible for the various IT environment aspects and assurance that the Town's IT system and data are properly safeguarded. Further, without a written agreement, officials do not have a clear understanding of the amount of compensation the IT consultant is entitled to or the extent of the services to be provided.

As a result, the Town's data and computer resources, including PPSI, are at a greater risk for unauthorized access, misuse or loss.

Why Should Town Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, town 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 and 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.[7] Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything 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.

Officials Did Not Provide IT Security Awareness Training

Town officials did not provide users with IT security awareness training to help ensure they understand IT security measures and their roles in safeguarding data and IT assets. As a result, IT assets and data were more vulnerable to loss and misuse. The Supervisor told us that he understands the importance of offering such training and is planning on providing training to all employees.

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

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

compromise IT assets. As a result, Town data and PPSI could be at greater risk for unauthorized access, misuse or loss.

What Do We Recommend?

The Board should:

1. Adopt comprehensive IT policies to address data classification, protection of PPSI, breach notification and data backups.

2. 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.

3. Enter into an SLA with the IT consultant for all IT services to be provided that sufficiently defines the roles and responsibilities of each party and addresses confidentiality and protection of PPSI.

Town officials should:

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

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

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

Appendix A: Response From Town Officials

SUPERVISOR
Richard Williams Sr.
Tel. (845) 878-6500
Fax. (845) 878-6343
supervisor@pattersonny.org

Susan Brown
Aide to the Town Board

TOWN COUNSEL
Hogan & Rossi
Tel. (845) 279-2986
Fax (845) 278-6135

TOWN OF PATTERSON
1142 Route 311
P.O. Box 470
Patterson, New York 12563
www.pattersonny.org

TOWN BOARD
Charles W. Cook
Peter Dandreano
Shawn Rogan
Mary E. Smith

TOWN CLERK
Eileen Fitzpatrick
Tel. (845) 878-6500
Fax (845 878-6343
townclerk@pattersonny.org

May 22, 2020

Ms. Lisa Reynolds
Office of the State Comptroller
Newburgh Regional Office
33 Airport Center Drive
Suite 103
New Windsor, NY 12553

Re: Report of Examination 20220M-37
Patterson Information Technology

Dear Ms. Reynolds:

The Town of Patterson has received the above-mentioned Draft Audit Report and intends this letter to serve as the Town's response. After review of the Draft Audit Report, the Town acknowledges the findings presented in the Report and intends to submit a corrective action plan addressing the key findings and recommendations found in the Report in the near future.

The Town of Patterson would like to thank the auditors for their time spent reviewing and identifying potential issues which may have affected the financial health of the Town. The auditors were professional and courteous, and were extremely helpful in assisting us in improving our financial practices. The Town recognizes the importance of the findings and is appreciative of the efforts the audit team made to discuss those findings and review corrective actions the Town might implement.

Sincerely yours,

Richard Williams Sr.
SUPERVISOR

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 Town's employee handbook and computer/network AUP to identify IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.
- We reviewed a list provided by the Town that showed the employees who signed acknowledgements stating that they had read the employee handbook and AUP. We selected a random sample of five employees of 162 employees during the audit period. We reviewed the acknowledgments for our sample to determine whether the list was accurate.
- 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 Town officials to gain an understanding of the IT environment and internal controls over IT assets.
- We used our professional judgment to select a sample of five computers from the Town's 40 computers. We selected computers of users who had access to PPSI and software programs with known vulnerabilities. We reviewed web history reports from these computers to evaluate whether Internet use was in compliance with the AUP guidelines.
- We ran a computerized audit script on our sample of five computers to analyze the Town's network information and determine whether user accounts were necessary. We reviewed user accounts and compared them to a list of current employees to determine whether any network users were no longer employed by the Town. We interviewed Town officials to determine the necessity of any such identified accounts.
- We ran a specialized shared folders audit script on our sample of five computers to identify any folders that could potentially have contained files that indicated misuse of Town computers. We then determined who had access to those folders and verified the contents of the folders with Town officials.

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 Town 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.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law. 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 Town Board to make the CAP available for public review in the Town 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

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, Rockland, Ulster, Westchester counties.

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