REPORT OF EXAMINATION | 2020M-16

Town of Yorktown

Information Technology

MAY 2020

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

Contents

Report Highlights

Town of Yorktown

Audit Objective

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

Key Findings

- Personal Internet use was found on computers assigned to 10 employees, including four who routinely accessed personal, private and sensitive information (PPSI).
- Town officials did not adequately manage user accounts.
- The Board did not develop a disaster recovery plan.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Provide adequate oversight of employee Internet use to ensure it complies with Board policies.
- Regularly review enabled user accounts and immediately disable user accounts when access is no longer needed.
- Develop and adopt a comprehensive disaster recovery plan, including backup procedures and offsite storage, and communicate the plan to officials and employees.

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

Background

The Town of Yorktown (Town) is located in Westchester County. The Town is governed by the Town Board (Board) which comprises four elected members and the Town Supervisor.

The Board is responsible for the general oversight of the Town's operations. The Supervisor is the Town's chief financial officer and chief executive officer and is responsible, along with other administrative staff, for the Town's day-to-day administration.

The Town contracted with an IT consultant to review and update the Town's computer systems to ensure system and hardware versions were current. The consultant also performed problem solving on an on-call basis.

Quick Facts	
Annual IT Contract	$73,250
Number of Computers	131
Network Accounts	210
Employees	564

Audit Period

January 1, 2018 – April 5, 2019. We extended our scope forward to August 14, 2019 to complete computer testing.

Information Technology

How Does an Acceptable Use Policy Secure and Protect the Town's IT Systems?

A town should have an acceptable use policy (AUP) that defines the procedures for computer, Internet and email use. The policy also should describe what constitutes appropriate and inappropriate use of IT resources and the board's expectations concerning personal use of IT equipment and user privacy.

Monitoring compliance with AUPs involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity. Officials should monitor and analyze activities for signs of possible violations or imminent threats of violations of computer security policies, AUPs or standard security practices.

Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability. Town officials can reduce the risks to personal, private and sensitive information (PPSI)[1] and IT assets by monitoring Internet usage and by developing and implementing procedures to ensure employee compliance with the AUP.

According to the Town's AUP,[2] users should and will use the Internet for work-related purposes only. For example, Internet use should be to communicate with employees, constituents, vendors, consultants and other government agencies; to research relevant topics; and obtain useful work-related information except as outlined below. Users are required to conduct themselves honestly and appropriately on the Internet. Also, users should not use the Town's IT system for any personal use.

Some Town Computers Were Used For Personal Activities

The Town had an AUP that defined proper procedures for using the Town's IT resources. However, Town officials did not design or implement procedures to monitor compliance with the policy or determine the amount of employees' personal use of Town computers.

We reviewed the web browsing history for 10 computers[3] used by 10 employees and found Internet use on all 10 computers that was not related to Town business-related purposes. This included social media use and accessing entertainment and leisure websites. Four of the 10 employees' job duties included routinely

1 Personal, private and sensitive information (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 The Town has an Information System Usage and Security Policy which serves as the AUP.

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

accessing PPSI. As a result, their personal Internet use unnecessarily exposed this information to possibly being compromised. Town officials were unaware of this personal computer use because they did not routinely monitor employee Internet use or have procedures designed to monitor IT usage and enforce compliance with the AUP.

Inappropriate or questionable use of Town computers could expose the Town to malicious software infections that compromise systems and data, including PPSI or ransomware attack. Also, when employees access websites for nonbusiness or inappropriate purposes through the Town's network, productivity is reduced.

Why Should the Town Manage User Accounts?

User accounts provide access to networks and financial applications 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 and in the financial system. A town should have a written policy and procedures for granting, changing and revoking access rights to the network.

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 or employees who have transferred to another area. The IT consultant is responsible to ensure user accounts for the IT system are managed in a timely and satisfactory manner.

Officials Did Not Adequately Manage User Accounts

Town officials did not develop comprehensive written procedures for managing system access and did not adequately manage user accounts for its network. As a result, we found that the Town had unneeded accounts that had not been disabled. During our review of all 210 network accounts, we found 13 accounts that did not match the employee master report or were unneeded.

Former Employees – When new employees were hired, Town officials provided the IT consultant with a form indicating the level of access that the new employees should be granted so they could be given a network user account. However, the Town did not have a formal process or written procedures for revoking user accounts.

Consequently, the IT consultant did not disable an employee's network account until he was notified by the Town that the employee had left the Town's employment. During our review of the 210 network accounts, we found enabled

network accounts for seven former employees. One of these former employees had left the Town's employment in December 2016. Officials told us they notified their IT consultant by email when employees left Town employment but were unaware that these accounts were not disabled. User accounts of former employees that have not been disabled or removed could potentially be used by those individuals or others for malicious purposes.

Unneeded Accounts – During our review of the 210 network accounts, we found five accounts that had originally been created for various uses that were no longer needed, including one account used to send emails and another related to installing software.

The IT consultant was unaware that these accounts were inactive. Because the Town did not have formal procedures for regularly reviewing enabled user accounts, the inactive user accounts went unnoticed until we brought them to officials' attention during our audit fieldwork. In addition, because they were not monitored, the Town had a greater risk that the IT consultant would not have noticed if the inactive accounts had been compromised or used for malicious purposes.

After we notified the IT consultant of the existence of the unneeded accounts, he disabled them. Officials must disable unnecessary accounts once there is no longer a need for them.

Why Should the Town Have a Disaster Recovery Plan?

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 ransomware attacks. The disaster recovery 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.

Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, identification of potential disasters, specific roles of key individuals and precautions needed to maintain or quickly resume operations. Additionally, a disaster recovery 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 and Town Officials Have Not Established a Disaster Recovery Plan

The Board did not adopt a formal written disaster recovery plan to establish how officials would respond to potential disasters. Consequently, in the event of a disaster, Town personnel have no guidance or plan to follow to restore or resume essential operations in a timely manner.

Town officials told us they were unaware of the need for a formal written disaster recovery plan because their financial data is backed up regularly, and backups are stored off-site. Because the Town does not have a disaster recovery plan that is specific to its IT environment, personnel have no guidelines to minimize the loss of IT equipment and data or implement data recovery in the event of a disaster.

Without a formal, written plan, the Town has an increased risk that it could lose important data and suffer serious interruption in operations, such as not being able to process checks to pay vendors or employees, or process daily Town Clerk functions.

What Do We Recommend?

Town officials should:

1. Monitor employee Internet usage and enforce the Town's AUP.
2. Develop written procedures for granting, changing and revoking access rights to the network.
3. Regularly review enabled user accounts and immediately disable user accounts when access is no longer needed.

The Board should:

4. Develop and adopt a comprehensive disaster recovery plan, including backup procedures and offsite storage, and communicate the plan to officials, employees and the IT consultant.

Appendix A: Response From Town Officials

Yorktown Town Hall
363 Underhill Avenue, P.O. Box 703
Yorktown Heights, NY 10598

(914) 962-5722
www.yorktownny.org

May 19, 2020

Office of the New York State Comptroller
Newburgh Regional Office
33 Airport Center Drive, Ste 103
New Windsor, NY 12553

Audit Report: Information Technology, Report of Examination
Audit Report Number: 2020M-16-IT

The Town of Yorktown is in receipt of and agrees with the findings of the draft audit report concerning Information Technology which was performed during 2019. Please accept this letter as the Town of Yorktown's response as well as the corrective action plan to this audit. The Town has reviewed the findings and recommendations and provides the following responses:

Office of State Comptroller Recommendations:
Recommendation:
Monitor employee Internet usage and enforce the Town's AUP
Response:
This was addressed and resolved during the audit process by working with the Town's IT consultant to make certain the Town's policy is not only followed but strictly adhered to

Recommendation:
Develop written procedures for granting, changing and revoking access rights to the network
Response:
This was addressed and resolved during the audit process by working with the Town's IT consultant to restrict the authorization of written requests for network access for employees to the Town Comptroller

Recommendation:
Regularly review enabled user accounts and immediately disable user accounts when access is no longer needed
Response:
This was addressed and resolved during the audit process by working with the Town's IT consultant to only accept written authorization of the Comptroller to disable employee access to the network upon the employee's separation or retirement from the Town

Recommendation:
Develop and adopt a comprehensive disaster recovery plan, including backup procedures and offsite storage and communicate the plan to officials, employees and the IT consultant
Response:
The Town is working with our IT consultants to elaborate on the current disaster recovery plan detailing each step involved in both backup and offsite storage processes. When finalized, this plan will be incorporated in the Town's policies and procedures and distributed to key employees.

We at the Town of Yorktown respect the professionalism of the auditor assigned and appreciate the recommendations for improvement.

Sincerely,

Matthew J Slater,
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 policy and procedure manuals to identify IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.
- We interviewed officials and personnel to gain an understanding of internal controls over IT and online banking.
- We ran a specialized audit script on the Town's domain controllers.[4] We then analyzed the reports to identify inactive user accounts.
- We used our professional judgment to select a sample of 10 out of 131 computers with 10 users. The 10 computers included three located in the Finance department, one in the Recreation department, one in the Building department, one in the Highway department, one in the Engineer department, one in the Supervisor office, one in the Receiver of taxes office and one in the Town Clerk office. The 10 users included three Finance department employees and one Town clerk department employee who all had access to key financial applications and related PPSI, including death and birth information for certificates to be issued, online banking, payroll and human resources data. The remaining employees worked in the Supervisor office, Recreation, Engineer, Building, Highway and Tax department. All had job duties and IT user privileges that involved using and transmitting electronic financial data. We reviewed web history reports on the 10 selected computers to identify names of websites accessed that could put the network at risk.
- We inquired about a disaster recovery plan.

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.

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

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 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 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