REPORT OF EXAMINATION | 2020M-89

Village of Red Hook

Information Technology

FEBRUARY 2021

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

Contents

Report Highlights

Village of Red Hook

Audit Objective

Determine whether Village of Red Hook (Village) officials ensured information technology (IT) systems were adequately secured and protected against unauthorized use, access and loss.

Key Findings

Officials did not adequately secure and protect the Village's IT systems against unauthorized use, access and loss.

- The Board did not adopt required or sufficient IT policies, provide users with IT security awareness training, or develop a disaster recovery plan.
- Officials were unaware that employees were accessing websites for nonbusiness purposes because they did not routinely monitor employee Internet use.
- The Village did not define the IT consultant's responsibilities and did not have a formal contract with the consultant.

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

Key Recommendations

- Develop and adopt comprehensive IT policies and provide employees with IT security awareness training.
- Develop procedures for monitoring Internet usage and negotiate a formal contract with the IT consultant.

Village officials generally agreed with our findings and recommendations and indicated they have initiated corrective action.

Background

The Village is located in the Town of Red Hook in Dutchess County. It is governed by an elected Board of Trustees (Board), which contains four trustees and the Village Mayor (Mayor).

The Board is responsible for oversight of Village operations. The Mayor is the chief executive officer and is responsible for the Village's day-to-day management, in addition to being a member of the Board.

The Village contracted with a third-party consultant (IT consultant) to maintain the Village's IT system.

Quick Facts	
Servers	2
Computers	9
Enabled Network Accounts	43
Employees	25

Audit Period

June 1, 2017 – October 11, 2018

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

A village 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, the village board's expectations concerning personal use of IT equipment and user privacy and the consequences for violating the policy.

Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability. Village officials can reduce the risks to personal, private and sensitive information (PPSI)[1] and IT assets by adopting an AUP and monitoring Internet usage. Officials also should develop and implement procedures to monitor employee compliance with the AUP.

Monitoring for AUP compliance 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 user activities for signs of possible violations or imminent threats of violations of the AUP, computer security policies and standard security practices.

The Board Did Not Adopt an AUP or Monitor Computer Use

The Board did not adopt an AUP governing appropriate and inappropriate use of Village IT resources. In addition, the Board and Village officials did not monitor employee Internet use for inappropriate or unusual activity.

We reviewed the web browsing history on four computers[2] and found questionable Internet use on three computers. This included online shopping, accessing personal email, browsing news and entertainment sites and music streaming.

Officials were unaware of this inappropriate computer use because they did not routinely monitor employee Internet use. In addition, the Board was unaware of the need for developing and communicating an AUP to employees and monitoring employee use of Village computers.

Because the Board and officials did not develop an AUP and monitor employee Internet use, the Village had an increased risk that valuable data, IT assets and any PPSI they contain could be exposed to damage and PPSI breach, loss or

> …[T]he Board and Village officials did not monitor employee Internet use for inappropriate or unusual activity.

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

misuse. In addition, when employees access websites for nonbusiness purposes through the network, it increases the likelihood of computers being exposed to malicious software that may compromise PPSI or expose the Village to ransomware attacks.

What Other IT Policies and Procedures Should the Board Adopt?

To ensure the highest level of security over village data, a board also should adopt policies and procedures for breach notification, data classification and the use of and access to PPSI. In addition, the board should develop a disaster recovery plan.

New York State Technology Law[3] requires local governments to adopt a breach notification policy that details actions to be taken to notify affected individuals if their personal information is compromised. The policy should address how officials would notify individuals whose private information was, or is reasonably believed to have been, acquired without valid authorization.

Data classification is the process of identifying and categorizing data to help officials make informed decisions about how to properly protect it. Data classification includes scanning data repositories and organizing the data to determine what it is, where it is located and how to protect it. Village officials should classify village data to properly identify where PPSI is stored and how to adequately protect it.

Classifying PPSI data and those who use it can help identify the type of security controls appropriate for safeguarding and disseminating the data. Policies covering the use of and access to PPSI should define PPSI, explain the entity's reasons for collecting PPSI and describe specific procedures for the access to and use, storage and disposal of PPSI involved in normal business activities.

To minimize the risk of data loss or suffering a serious interruption of services, village officials should establish a formal, written disaster recovery plan (plan)[4] to anticipate and plan for IT disruptions involving the corruption or loss of data and for other problematic events. This is particularly important given the current and growing threat of ransomware attack. The plan should address the potential for sudden, unplanned catastrophic events (e.g., fire, flood, computer virus, vandalism, or inadvertent employee action) that could compromise the network and the availability or integrity of computer systems and any PPSI contained therein.

…Village officials should establish a formal, written disaster recovery plan to anticipate and plan for IT disruptions involving the corruption or loss of data….

3 New York State Technology Law Section 208

4 Also referred to as a business continuity plan or business process contingency plan

Typically, a plan involves analyzing business processes and continuity needs, focusing on disaster prevention and identifying roles of key individuals and necessary procedures to follow to maintain or quickly resume operations. The plan should be tested periodically and updated to ensure officials understand their roles and responsibilities in a disaster situation and to address changes in security requirements.

A disaster recovery plan also should include data backup[5] procedures to help ensure that data are routinely backed up. The procedures should require backups to be stored at a secure offsite location, encrypted and periodically tested to ensure its integrity and that it 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 Did Not Adopt Sufficient IT Policies or Procedures

The Board did not adopt policies and procedures for breach notification, data classification or the use of and access to PPSI. Also, the Board did not establish a disaster recovery plan. However, Village personnel performed data backups, which were encrypted, stored the backups offsite and periodically tested them.

The Mayor told us that the Village had cybersecurity coverage through its insurance policy, which would help notify individuals in the event of a breach. However, the Board did not consider developing and adopting breach notification, data classification and use of and access to PPSI policies.

Without these policies, officials cannot ensure that employees are aware of their responsibilities for safeguarding sensitive information. Also, the Village might not be able to fulfill its legal obligation to notify affected individuals if PPSI is compromised.

Furthermore, in the event of a disaster, Village personnel have no guidelines or plan to follow to prevent the loss of equipment and data or appropriately recover data. Although appropriate backup procedures can help ensure data is not lost, without a formal written plan, responsible parties might not be aware of steps they should take, or how to continue performing their jobs, to resume business after a disruptive event.

As a result, the Village could experience a serious interruption to its operations, such as not being able to process payroll or vendor claims, and its IT assets could be vulnerable to loss and misuse.

The Mayor told us that the Village had cybersecurity coverage through its insurance policy, which would help notify individuals in the event of a breach.

5 A backup is a copy of data files and software programs made to replace original versions if there is loss or damage to the original.

Why Should the Village Manage User Accounts?

Computer networks[6] can be accessed by network user accounts, which identify specific users. Network user accounts provide access to network resources and should be actively managed to minimize the risk of unauthorized access and misuse. If user accounts are not properly managed, they could be potential entry points for attackers because they could be used to inappropriately access and view PPSI on the network.

Effective user account management includes managing the creation, use and dormancy of user accounts and regularly reviewing them to ensure they are still needed. When employees leave village employment or when user accounts are otherwise no longer needed, officials must disable these accounts in a timely manner. A village should have a written policy and procedures for granting, changing and revoking users' access to the network.

Officials Did Not Adequately Manage User Accounts

Village officials did not develop comprehensive written procedures for managing network access and did not adequately manage user accounts for its network. During our review of all 43 network accounts, we found enabled network accounts for eight former employees. One of these former employees had left Village employment in July 2012.

Officials could not provide a reason for why these accounts were still active at the time of our review. However, the Mayor told us the accounts have since been 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.

Why Should the Village Provide IT Security Awareness Training to Employees?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, village 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, this training should communicate IT policies and procedures and the disaster recovery plan to all employees and IT staff.

The training should center on emerging trends such as information theft, social engineering attacks[7] and computer viruses and other types of malicious software, all of which may block access to the IT system and its data or result in PPSI

The training should center on emerging trends such as information theft, social engineering attacks and computer viruses and other types of malicious software….

6 A group of two or more connected computers

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

compromise. 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 downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems.

Village Employees Were Not Provided With IT Security Awareness Training

The Village did not provide employees with IT security awareness training to help ensure they understand IT security measures needed to protect the Village's IT system. The Mayor told us employees received some training that addressed not clicking on unknown links in emails.

However, this training did not cover all aspects of IT security awareness. For example, the training did not include the importance of selecting strong passwords, acceptable computer use or the risks involved with using unsecured Wi-Fi connections. As a result, employees might not have been aware of the risks associated with using the Village's IT system and could have inadvertently exposed the Village's IT assets to cybersecurity attacks, loss and misuse.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. Village officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that users, or those who manage IT, understand the IT security policies and procedures and their roles and responsibilities related to IT and data security.

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

What Should Be Included in an IT Consulting Contract?

Village officials must ensure that they have qualified IT personnel to manage the village's IT environment. This can be accomplished by using village employees, an IT service provider (IT consultant) or both.

A written contract provides both parties with a clear understanding of the services expected to be provided and a legal basis for compensation provided for those services. To avoid potential misunderstandings and to protect village assets, officials should have a written agreement between the village and its IT consultant

that clearly states the village's needs and service expectations. The agreement must include provisions relating to confidentiality and protection of PPSI and specify the level of service to be provided.

The Village Did Not Have a Contract With Its IT Consultant

Village officials relied on an IT consultant for the Village's IT services and technical assistance, as needed. However, the Board did not negotiate a formal contract with the IT consultant that identified specific services to be provided or the IT consultant's responsibilities.

The Mayor told us the Village had an agreement with the IT consultant regarding how much the Village would pay the IT consultant. However, the Mayor could not explain why the Village did not have a formal contract with the IT consultant. After we completed our audit fieldwork, the Village replaced the IT consultant and entered into a formal contract with a new consultant.

Without a formal contract, the roles and responsibilities of each party are undefined. Also, without clearly defined roles and responsibilities, gaps in IT security practices could occur. When essential IT security tasks – such as monitoring Internet usage and managing user accounts – are not performed, it could put the Village's IT assets and data at greater risk for unauthorized access, misuse or loss.

Each of the weaknesses discussed in this report exposed the Village to an increased risk of a data breach or compromise, or of malware such as ransomware being installed on the Village's network that could block access to its IT system and data.

However, it is important to note that the Village's multiple weaknesses have a compounding effect. For example, unrestricted Internet browsing makes users more likely to be attacked and, without IT security training, users are more susceptible to the attacks. Given the current prevalence of ransomware attacks against municipalities, it is important for the Village to develop a comprehensive set of policies and procedures to protect its IT system.

What Do We Recommend?

The Board should:

1. Develop and adopt comprehensive IT policies to address acceptable computer use, breach notification, data classification and the use of and access to PPSI.

2. Develop and adopt a comprehensive disaster recovery plan and communicate the plan to officials, employees and the IT consultant.

3. Enter into a professional service contract with the IT consultant that sufficiently defines the roles and responsibilities of each party, includes all services to be provided and addresses confidentiality and protection of PPSI.

Village officials should:

4. Develop procedures for monitoring employee Internet use and managing network access.

5. Regularly review enabled user accounts and ensure that unneeded user accounts are immediately disabled.

6. Ensure that employees receive formal IT security awareness training on an on-going basis that reflects current risks identified by the IT community and includes training on all IT policies.

Appendix A: Response From Village Officials

VILLAGE OF RED HOOK

Building & Zoning Dept.

7467 SOUTH BROADWAY
RED HOOK, NY 12571

Office (845) 758-1081
Fax (845) 758-5460
zoning@redhooknyvillage.org

January 7, 2021

State of New York
Office of the State Comptroller
110 State Street
Albany, NY 12236

Re: Village of Red Hook Audit 2020M-89-IT

Dear Mr. Auerbach:

On December 9, 2020 we received the IT audit noted above and later had an exit interview with staff from your office regarding their audit.

We have taken many positive steps since the actual auditor was on site and point out that the audit examined a time period of June 1, 2017 through October 11, 2018. We had preliminary talks with the on-site auditor and your staff back in that late 2018 timeframe and we've made various changes and upgrades with regard to items mentioned back then.

Now that we have the actual written audit report, here is our response which will also serve as our corrective action plan:

The Village of Red Hook has a population of 2,000 folks and is a vibrant and modern place. The village government designed to be effective and efficient but is a relatively small operation. Although the audit over-view illustration lists 25 employees, that is a composite of many part-time employees. We only have five employees that use computer workstations plus four car-mounted police laptops linked to NYSP and two tablets. We have no in-house IT Department nor any employee skilled enough to be able to design and operate our IT system. Therefore, we rely on outside, paid professional consultants in conjunction with the specific vendors whose software we utilize. Back at the time of the audit we had an IT services agreement with an individual but since then moved into a written contract agreement with a new firm, [redacted] This written contract was negotiated and includes block of time allocations that are at double

the hourly rate of the prior scenario and remains in force today. The new vendor is very skilled, responsive and has a deeper staff. They work with us on policy and process as well as hardware and software needs but we are still guided by the expertise of outside entities.

In the interim, we have developed a Social Media, Internet and Website Policy and will include the topic in our annual staff meetings and will periodically remind our staff of the problems of malware and email security awareness. Restricting staff access to web-based sites will be considered but access to the web is part of day to day operations. We already had the new IT firm review and update the user accounts record. We will work with them when there are staff turn-overs and keep the user list current. It is our position that we have a disaster work/recovery plan, without getting into too many specifics here, that is developed and managed by our IT consultant. The Village also purchased specific cyber insurance coverage in our package policy which helps on many aspects in this area.

We will circulate the December 9, 2020 recommendations to our vendor, in particular the six recommendations. But, as this response indicates, we have already addressed many of the items and we work closely with them on any open items.

In this new covid19 era we have converted certain operations and tasks to remote and on-line processes and created a pandemic operations mode that worked and we were able to deliver services. Each step we take is coordinated with our IT vendor and the particular software vendor to comply with protocols and security.

Since the onset of the tax cap law, this village has kept its levy within the cap, year in and year out. This year we begin our budget planning with a 1.31% goal, which will affect all parts of our operation, including our IT operations.

We will continue to work with your office and the recommendations made in the audit for the future of a better Red Hook.

Very truly yours,

Ed Blundell
Mayor

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, we performed the following audit procedures:

- We reviewed Board minutes and Village policies to identify IT-related policies and evaluated those policies to gain an understanding of internal controls over IT.
- We interviewed Village officials to gain an understanding of the processes of and procedures for the IT systems.
- We ran a specialized audit script on the Village's domain controller.[8] We then compared the Village's master payroll list to IT users listed in the reports to determine whether any users who were no longer employed by the Village still had active accounts and identify unneeded user accounts.
- We used our professional judgment to select a sample of four out of nine desktop computers used by Village employees. The four computers included two from the Clerk's Office and two in the Zoning Department. We reviewed Internet history reports on the four selected computers to identify names of websites accessed that could put the network at risk. We eliminated three remaining Village computers in the Village's Police Department from our testing sample because employees in this department regularly needed to access nonbusiness websites in the normal course of their duties. As a result, this Internet usage would have been identified as improper usage during our testing. We also eliminated the remaining two Village computers in the Village Justice Court from our testing sample because OSC recently audited the Town of Red Hook without finding any significant IT discrepancies, the Village Justice is also the Town Justice and access to the two computers was limited to Court personnel.

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 Village officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). 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.

8 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.

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 Board to make the CAP available for public review in the Village Clerk's office.

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, Rockland, Ulster, Westchester counties

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