REPORT OF EXAMINATION | 2019M-203

Village of Arkport

Information Technology

JANUARY 2020

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

Contents

Report Highlights

Village of Arkport

Audit Objective

Determine whether Village officials adequately safeguarded Village information technology (IT) assets.

Key Findings

The Board did not:

- Develop adequate IT policies and procedures.
- Enter into a written agreement with the IT vendor for services provided to the Village.
- Provide IT security awareness training to employees.

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

Key Recommendations

The Board should:

- Adopt comprehensive IT security policies, periodically review and update all IT policies and procedures to reflect changes in technology and the Village's computing environment, and stipulate who is responsible for monitoring all IT policies.
- Enter into a professional service contract with the IT vendor that sufficiently defines the role and responsibilities of each party, includes all services to be provided, and addresses confidentiality and protection of personal, private and sensitive information (PPSI).
- Provide periodic IT security awareness training to personnel who use IT resources, including the importance of maintaining physical security and protecting PPSI.

District officials generally agreed with our findings and indicated they plan to initiate corrective action.

Background

The Village of Arkport (Village) is located in the Town of Hornellsville in Steuben County. The Village is governed by a Board of Trustees (Board), which is composed of an elected Mayor and four elected Trustees.

Village officials and employees use IT to initiate, process, record and report financial transactions, Internet access and email. The Treasurer uses Internet access for authorizing online banking transactions and submitting required reports.

The Village works with an IT vendor to perform all IT services for the Village, such as setting up new computers and troubleshooting computer issues. The Village has an internal network that allows individuals to share and access electronic data and computer resources. The IT vendor also manages the Village's network security and the data it contains.

Quick Facts	
Desktop Computers	3
Number of Employees	11
2019-20 Total Village Appropriations	$698,821

Audit Period

June 1, 2018 – October 1, 2019

Information Technology

What Policies and Procedures Should the Board Adopt to Safeguard Village IT Assets?

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. Therefore, it is essential for a board to establish security policies for key IT security issues.

The board should have acceptable computer use policies that define specific consequences for violations and address security awareness. Additionally, the board should establish computer policies that take into account people, processes and technology and communicate them throughout the village.[1] New York State Technology Law requires municipalities and other local agencies to have a breach notification policy that requires notification be given to certain individuals in the event of a system security breach, as it relates to private information. Finally, 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 IT Security Policies and Procedures

The Board did not adopt IT security policies and procedures addressing key IT security issues, such as those related to acceptable use, online banking, password security use of and access to personal private and sensitive information (PPSI), and breach notification. The Board also has not adopted a comprehensive disaster recovery plan. Therefore, IT vendors and employees did not have guidance related to the appropriate use of Village IT assets. Consequently, IT assets are at risk for unauthorized, inappropriate and wasteful use, and the Village could incur a potentially costly disruption of operations and services.

While IT policies will not guarantee the safety of the Village's systems, a lack of appropriate policies significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate use or access. Without formal policies that explicitly convey the appropriate use of the Village's computer equipment and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities.

What Should Be Included in an IT Vendor 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 vendor) or both. To avoid potential misunderstandings and to protect village assets, the village should have a written agreement with its

1 Refer to our publication *Information Technology Governance* available at http://www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf

IT vendor 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 Board Did Not Contract with the IT Vendor

Village officials relied on an IT vender for IT services and technical assistance, as needed. The IT vendor stated it was a "break/fix relationship."[2] Therefore, the IT vendor did not perform critical maintenance tasks on a regular basis. Without a contract, the roles and responsibilities of each party are not defined. The lack of a written agreement put the Village's IT assets and data at greater risk for unauthorized access, misuse or loss.

How Can Village Officials Reduce the Risk of Inappropriate Online Banking Transactions?

Online banking provides a means of direct access to funds held in village accounts. Users can review current account balances and account information, including recent transactions, and transfer money between bank accounts and to external accounts. Because wire transfers of funds typically involve significant amounts of money, villages must control the processing of their wire transfers to help prevent unauthorized transfers from occurring. It is essential that village officials authorize transfers before they are initiated and establish procedures to ensure that employees are securely accessing banking websites to help reduce the risk of unauthorized transfers from both internal and external sources.

To safeguard cash assets, a board must adopt policies and procedures to properly monitor and control online banking transactions. A comprehensive written online banking policy clearly describes the online activities village officials will engage in, specifies which employees are authorized to process transactions and establishes a detailed approval process to verify the accuracy and legitimacy of transfer requests. Officials must properly segregate the duties of employees granted access to the online banking applications to ensure that employees are unable to perform all financial transactions on their own. Segregation of duties should include bank accounts being monitored for unauthorized or suspicious activity at least every two or three days.

Good management practices require limiting the number of users authorized to execute online banking activities and the number of computers used. Banking agreements should identify current authorized users, and authorized online banking users should access bank accounts from one computer dedicated for online banking transactions. This will minimize exposure to malicious software

2 A "break/fix relationship" means that when the Village's equipment needs repairs, Village officials contact the vendor for assistance. Otherwise, the vendor does not come onsite regularly to provide maintenance.

because the other computers are used for activities that may introduce additional risk to the computers' integrity, and transactions executed from those computers could be more at risk.

Village Officials Did Not Safeguard Online Banking Transactions

Because the Board did not adopt an online banking policy, authorized users were not identified and a detailed approval process to verify the accuracy and legitimacy of online banking transactions was not established. Village officials did not adequately segregate online banking duties, ensure authorized access to bank accounts was limited, or maintain up-to-date and adequate banking agreements. Officials also did not use a dedicated separate computer for these transactions or prohibit personal computer use.

The Treasurer performs online banking transactions at two banks using her own usernames and passwords. One of the banks also assigned her a security token[3] for performing online banking transactions. The Treasurer initiates transfers between the Village's bank accounts and initiates automated clearing house (ACH) transactions on the same computer that she performs all her other Treasurer's duties and Internet browsing.

The use of the token limited unauthorized access from outside sources at the one bank. However, the Treasurer performed online banking transactions with no oversight because the Village's outdated banking agreements did not establish adequate security controls. Such controls could include requiring secondary authorizations for online transfers, wire transfers and ACH transactions. Further, access to the Treasurer's computer and credentials was not limited and sufficiently secured. The Treasurer stated this was so that Board members and the Clerk could access the Treasurer's online banking and the Village's financial records to perform reviews. However, the Deputy Mayor stated that the Treasurer is the only individual set up and accessing online banking. Therefore, the Board and Clerk were not reviewing the online banking to justify the added risks associated with the Treasurer providing this access.

The lack of segregation of duties and access controls to online banking increase the risk that unauthorized individuals could access the Village's bank accounts and misappropriate funds.

Why Should the Village Provide IT Security Awareness Training?

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

3 Token identifications contain a number series assigned to a specific user.

and data and communicates related policies and procedures to all employees. The training should center on emerging trends such as information theft, social engineering attacks[4] and computer viruses and other types of malicious software, all of which may result in PPSI compromise. Training programs should be directed at the specific audience (e.g., system users) and include everything that attendees need to perform their jobs, such as secure online banking for users who perform online banking transactions.

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.

Village Employees Were Not Provided IT Security Awareness Training

Village officials and employees were not provided IT security awareness training to help ensure they understood IT security measures designed to safeguard online activity. 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, online banking transactions, Village financial data and PPSI could be at a greater risk for unauthorized access, misuse or abuse.

Because Village officials and employees were not provided IT security awareness training, we reviewed the website browsing histories on the three Village computers[5] and did not identify any questionable personal use. However, not prohibiting personal use of computers increases the risk of malicious software and attacks on the computer system and can decrease employee productivity.

What Are Strong Access Controls?

Computer access controls prescribe which computer users may have access to a specific computer resource, such as a particular software program or database. There should be written procedures in place for granting, changing

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

5 The Treasurer's and Clerk's computers did not have any website browsing histories to review, as their computer settings were set to delete browsing history after one hour.

and terminating access rights to the overall networked computer system and to specific software applications. Access rights should be updated as necessary. Inactive, retired or terminated accounts should be disabled in a timely manner.

To help ensure individual accountability within the network, each user should have his or her own network account (username and password). Likewise, to help ensure individual accountability within software applications, each user should have his or her own user account (username and password). If users share accounts, accountability is diminished and activity in the system may not be able to be traced back to a single user.

Village Officials Did Not Implement Strong Access Controls

Village officials have not implemented comprehensive procedures for managing, limiting, securing and monitoring user access. The Clerk's and Treasurer's computers are networked and the Department of Public Works Superintendent uses a stand-alone computer. The IT vendor centrally manages and administers access to the internal network and associated resources for the Clerk's and Treasurer's computers in the Village office. Within this environment (domain), a domain controller facilitates user management and defines global security, access and privilege rights. Our review of network user accounts and settings, enforced policies and user account information found officials did not adequately manage user accounts.

We identified 16 network user accounts, many of which were unneeded. Specifically, 13 (81 percent) of the network user accounts have not been used in the last six months and four (25 percent) of these were assigned to former employees. Village officials agreed that many of these accounts were no longer needed.

In addition, the Treasurer used two financial software applications to process financial transactions. The Treasurer shared each of her user accounts' credentials for these applications with other Village officials. Because multiple users share user account credentials, any suspicious activity could not be traced to a single user. Consequently, the Village's IT assets are at increased risk for loss or misuse.

What Do We Recommend?

The Board should:

1. Adopt comprehensive IT security policies addressing password security, use of and access to PPSI, online banking, acceptable computer use and breach notification.

2. Periodically review and update all IT policies and procedures to reflect changes in technology and the Village's computing environment and stipulate who is responsible for monitoring all IT policies.

3. Develop and adopt a comprehensive disaster recovery plan, including adequate backup procedures and offsite storage.

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

5. Ensure banking agreements reflect current operations and provide for adequate controls over online banking transactions.

6. Provide periodic IT security awareness training to Village officials and employees who use IT resources, including the importance of physical security and protection of PPSI.

Village officials should:

7. Develop procedures to adequately segregate online banking duties, outline approved online banking activities (including accessing and exiting the online banking website) and assign responsibility for ensuring that the transactions are conducted safely and monitored.

8. Enable notifications and other security measures available from the bank, including secondary approvals and email notifications every time an online transaction occurs.

9. Consider designating a computer to be used for online banking transactions.

10. Develop comprehensive written procedures for granting, changing and terminating access rights to the overall networked computer system and to specific software applications.

11. Ensure access rights are monitored and updated as necessary. Disable inactive, retired or terminated accounts in a timely manner.

12. Ensure each user has his or her own unique account (username and password) for both network, online and software access.

Appendix A: Response From Village Officials

Village of Arkport
Arkport NY 14807

Mayor:
Charles W. Flanders

Attorney for Village:
John Vogel

6 Park Avenue, PO Box 465
Arkport, NY 14807-0465
Phone: (607) 295-7346
Fax: (607) 295-8648
arkport.village@gmail.com

Trustees:
Ryan Beers
Michael Brewer
Ezra Geist
Jon Hedges

Office of the New York State Comptroller
Division of Local Government and School Accountability
PSU-CAP Submission
110 State Street, 12th Floor
Albany, New York 12236

We, the Village of Arkport Board of Trustees, welcomes the Audit from New York State Comptroller's Office and agrees with the findings of the Audit.

It is the Village of Arkport's intent to address and abide by every recommendation that the Audit team has provided to the Village and including the following plans of action.

1) The Village of Arkport Board of Trustees created and adopted a Comprehensive IT Security Policy and Procedures during our December Village Board Meeting
2) The Village of Arkport Board of Trustees agrees to review and update all of our IT policies and procedures reflecting the changes in technology and the Village computing environment including who is responsible for monitoring all IT procedures.
3) Once the Village of Arkport Board of Trustees has an agreement with approved IT Vendor (see statement # 4) – with the guidance and direction of the IT Vendor the Village Board will adopt a comprehensive disaster recovery plan including adequate back up procedures and offsite storage.
4) The Village of Arkport is in the process of agreeing to professional service contract with an approved IT Vendor which will define the role and responsibilities of both parties which will include all services to be provided and addressing confidentiality and protection of PPSI.
5) The Village of Arkport will ensure that all banking agreements reflect current operations and provide adequate controls over online banking transactions.
6) The Village of Arkport will provide access to periodic IT security awareness training- including Internal Training and / or approved NY State Training.

Village of Arkport Board of Trustees
Deputy Mayor

Jon Hedges

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 interviewed Village officials and the IT vendor to obtain an understanding of IT operations and to obtain any related policies and procedures.
- We examined the Village's network user accounts and settings using specialized audit script. We compared the network user accounts to current employees to identify inactive and unnecessary accounts.
- We observed the Treasurer accessing online banking from logon to logoff.
- We inquired about a written agreement with the bank and reviewed the documentation regarding capabilities for electronic transfers.
- We examined the three Village computers using specialized audit script to obtain web histories and installed software and device settings. We reviewed the device settings for these computers.
- During the performance of our testing, we walked throughout the Village's facilities and made observations of physical security controls.

Our audit also examined the adequacy of certain IT 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 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.

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 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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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