REPORT OF EXAMINATION | 2017M-293

City of Hornell

Information Technology

MARCH 2018

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

Contents

Report Highlights

City of Hornell

Audit Objective

Determine whether the City adequately secured and safeguarded its computerized data.

Key Findings

- The Council and City officials did not develop adequate information technology (IT) policies and procedures to address acceptable use, sanitization and disposal and breach notification.
- City officials did not provide IT security awareness training for City employees.
- The Council did not develop a disaster recovery plan.

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

Key Recommendations

- The Council should adopt written IT policies and procedures to address acceptable use, sanitization and disposal and breach notification.
- The Council should provide users with IT security awareness training to help ensure they understand security measures that protect the network.
- The Council should adopt a disaster recovery plan to describe how City officials will manage potential disasters that affect the IT system.

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

Background

The City of Hornell (City) is located in Steuben County and has a population of approximately 8,500. The City is governed by a charter, State statutes and local laws and ordinances. The City's charter outlines the powers and duties of the Common Council (Council), Mayor and City Chamberlain.

The 10-member Council is the City's legislative branch. The Mayor is the City's chief executive officer and administrative officer and is generally responsible for the administration and supervision of City affairs. The elected City Chamberlain is responsible for supervising the City's fiscal affairs.

Quick Facts	
2017-18 Budgeted City Appropriations	$13 million
# of City Computers	48
# of Employees	149
IT Vendor Annual Retainer	$21,000

Audit Period

April 1, 2015 – October 2, 2017

Information Technology

The City uses IT to initiate, process, record and report transactions. It also relies on its IT systems for Internet access, email and maintaining financial information. The City has an internal network that allows individuals to share and access electronic data and computer resources. The City contracts with an IT vendor to perform all IT services for the City, such as setting up new computers and network access and troubleshooting network problems.

Which Policies and Procedures Should the Council Adopt to Safeguard City IT Data?

An effective process for safeguarding the City's IT system includes an acceptable computer use policy that defines the procedures for computer, Internet and email use and holds users accountable for properly using and protecting City resources. The acceptable use policy should also include IT security awareness training requirements for staff.

Additionally, the Council should adopt policies and procedures for granting, revoking, modifying and monitoring individual access rights and a process to monitor and review these rights once granted. To ensure the highest level of security over City data, the Council should also adopt policies and procedures for electronic media sanitation and disposal and security management.

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. The policy should detail how officials would notify individuals whose private information was, or is reasonably believed to have been, acquired without valid authorization. The disclosure should be made in the most expedient time possible consistent with legitimate needs of law enforcement or any measure necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Finally, all IT policies and procedures should be periodically reviewed and updated to reflect changes in technology and the City's computing environment.

The Council Did Not Adopt Adequate IT Security Policies and Procedures

While the City has an acceptable use policy, it is inadequate and not monitored or enforced. The policy does not address connecting personal devices to the City's network and does not specify penalties for noncompliance. Connecting personal devices to the City's network can create vulnerabilities in security and allow inappropriate access to City data. Employees need to be aware of these risks.

However, the City has not provided security awareness training to staff,[1] and the acceptable use policy did not address training requirements.

We reviewed installed programs on 17 City computers[2] and found 773 installed programs, most of which were acceptable. However, we found 46 questionable programs (6 percent), including games, iTunes and personal tax software.

The Board has not adopted a sanitization and disposal policy. Currently, the City retains outdated computers in the server room until they are recycled annually. While the IT vendor removes hard drives prior to recycling, they are left in the server room without a plan for sanitization and disposal.

Additionally, the Council has not adopted a breach notification policy. If private information is compromised, without an information breach notification policy City officials and employees may not be prepared to notify affected individuals.

While IT policies will not guarantee the safety of the City'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 City'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?

City officials must ensure that they have qualified IT personnel to manage the City's IT environment. This can be accomplished by using City employees, an IT service provider (IT vendor) or both. To avoid potential misunderstandings and to protect City assets, the City should have a written agreement with its IT vendor that clearly states the City's needs and service expectations. The agreement must include provisions relating to confidentiality and protection of personal, private and sensitive data and specify the level of service to be provided.

The Council Did Not Adopt an Adequate Contract With the IT Vendor

The City relied on an IT vendor for IT services and technical assistance, as needed. Although the City has a retainer services agreement (agreement) with the IT vendor, the agreement does not sufficiently define the roles and responsibilities for each party or include the type of services provided. The agreement also does not address confidentiality or protection of personal, private and sensitive data. Insufficient or vague agreements can contribute to confusion over who is responsible for various aspects of the IT environment, which puts the City's data and computer resources at greater risk for unauthorized access, misuse or loss.

1 Refer to "Why Should City Officials Provide IT Security Awareness Training?" for further information.

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

Why Should City Officials Provide IT Security Awareness Training?

Computer users must be aware of security risks and trained in practices that reduce internal and external threats to IT systems and data. While IT policies tell computer users what to do, IT security awareness training helps them understand their roles and responsibilities and provides them with the skills to perform them.

Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything that attendees need to perform their jobs. IT security awareness should reinforce IT policies and can focus on security in general or a more narrow aspect of security (e.g., the dangers of opening an unknown email or attachment or how to maintain laptop security while traveling).

City Officials Did Not Provide IT Security Awareness Training

City officials did not provide users with IT security awareness training to help ensure they understand security measures to protect the network. As a result, the City's IT assets are more vulnerable to loss and misuse.

Why Should the City Have a Disaster Recovery Plan?

A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. Disasters may include any sudden, catastrophic event[3] that compromises the availability or integrity of an IT system and data. Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, disaster prevention instructions, specific roles of key individuals and precautions needed to maintain or quickly resume operations. Additionally, a disaster recovery plan should include data backup procedures and periodic backup testing to ensure they will function as expected.

The City Does Not Have a Disaster Recovery Plan

The City does not have a disaster recovery plan. If IT systems are compromised, the results could range from inconvenience to catastrophe and could require extensive effort and financial resources to evaluate and repair.

3 Such as a fire, computer virus or inadvertent employee action

Why Should the City Maintain IT Hardware and Software Inventory Records?

City officials should maintain detailed, up-to-date inventory records for all computer hardware and software to safeguard IT assets. Information maintained for each piece of computer equipment should include a description of the item, name of the employee to whom the equipment is assigned, physical location of the equipment and relevant purchase or lease information. Officials should verify the accuracy of inventory records through periodic physical inventory counts.

The management of software and licenses is essential to safeguarding assets and data. Therefore, City officials must be aware of the software owned by the City, how it is used and how best to track user rights to ensure licensing compliance. Software inventory records should include software application descriptions, versions and serial numbers; description and location of computers on which the software is installed; and pertinent licensing information. Effective software management also includes ensuring that only appropriate business software is installed to reduce the risk of unwanted consequences and unnecessary costs that could result from unauthorized software. Additionally, City officials must ensure that software and patches are up to date to reduce vulnerabilities.

Complex IT environments must have a documented network topology, which is a map of the IT network's "nodes" (computers, printers, routers and other devices) and "links" (descriptions of how the nodes are connected to the network, such as by copper or fiber-optic cables). A documented network topology helps employees determine how the network is wired and configured to diagnose connectivity issues and perform capacity planning and network maintenance and expansion.

City Officials Did Not Maintain IT Inventory Records

We found that City officials did not maintain an inventory of the City's IT equipment, including computers and hard drives or installed software applications. Additionally, City officials did not maintain a documented network topology.

Organizations cannot properly protect IT resources if personnel are unaware of existing resources and where those resources reside. Because City officials did not maintain detailed, up-to-date hardware and software inventory records, the City has an increased risk that its IT assets may be lost, stolen or misused. Without a complete and comprehensive software inventory, the Board cannot ensure that all software programs running on City computers are properly licensed and for legitimate business purposes.

What Do We Recommend?

The Council should:

1. Update the acceptable use policy to address penalties for noncompliance and connecting personal devices to the City's network and include IT security awareness training requirements.

2. Adopt written IT policies and procedures to address media sanitization and disposal, breach notification and disaster recovery.

3. 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 data.

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

City officials should:

5. Monitor installed software programs on all City computers to ensure the programs serve an appropriate business purpose.

6. Develop a plan to sanitize and dispose outdated hard drives as soon as equipment is taken out of service.

7. Provide IT security awareness training to personnel who use IT resources.

8. Ensure IT backup procedures and the backups themselves function properly.

9. Develop and maintain adequate, up-to-date inventories of IT hardware and software assets.

10. Maintain a documented network topology.

Appendix A: Response From City Officials

CITY OF HORNELL
82 Main Street, PO Box 627, Hornell, NY 14843
(607) 324-7421 • (607)324-3150 Fax

March 7, 2018

Edward V. Grant, Jr.
Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, NY 14614

RE: Response to Preliminary Draft Findings

Dear Mr. Grant:

I am writing on behalf of the City of Hornell in response to the preliminary draft findings regarding your recent audit of our Information Technology Department.

We agree that the key findings are issues that need to be addressed. I am forming a "Policies and Procedures Committee" within our Common Council and these problems will certainly be at the top of the list. Additionally, we will be working closely with our IT provider to fix the faults in our security controls.

I appreciate your office's suggestions and recommendations as to how we can improve our IT operations and security. We take this very seriously and will certainly be working to remedy any weaknesses.

Thank you and your staff for your time and efforts. It was a pleasure working with your team.

Sincerely,

John J. Buckley
Mayor

JJB/bp

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 Council meeting minutes and interviewed City officials and the IT vendor to gain an understanding of the City's IT operations.
- We reviewed the City's IT vendor contract.
- We examined two computers from each department, except for the Assessor office which only had one computer, for a total of 17 computers. We used WinAudit during our examination and reviewed the results for inappropriate software programs, such as games.

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 City 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.

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 Common Council to make the CAP available for public review in the City 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/lgli/pdf/cybersecurityguide.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.state.ny.us

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.state.ny.us

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