OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Software Management

2015-MR-3

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

September 2015

Dear College Officials:

A top priority of the Office of the State Comptroller is to help local government officials manage government resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of local governments statewide, as well as compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations and Board of Trustee governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard local government assets.

Following is a report of our audit titled Software Management. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of New York State General Municipal Law.

This audit's results and recommendations are resources for local government officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

State of New York
Office of the State Comptroller

EXECUTIVE SUMMARY

Software assets have become increasingly important to local governments. Not only are they a vital element of information technology (IT) services that enable business-critical processes, but they also represent a large proportion of IT costs. Local governments also risk potential fines and penalties for using software applications that are not properly licensed. Additionally, local governments risk significant payroll overtime, consulting fees and equipment costs when unapproved or non-authentic software is installed on their networks, introducing unwanted, uninvited and often unintended consequences such as unforeseen crashes, breaches or system failures. Therefore, local governments need an understanding of the software they own, how it is used and how best to track user rights to ensure licensing compliance. Additionally, websites and related supporting servers are also an area of significance as attackers could identify vulnerabilities and use them to their advantage to gain unauthorized access to a network, possibly exposing a network or data to security threats. Strong website and related network security could result in decreased intrusions on a system and risks associated with data breaches.

Software management and website security are of particular importance to larger local governments, such as colleges, that have many different users[1] that perform a variety of functions. Typically, colleges will have several software applications and multiple licenses for each.

The three colleges (Colleges) we audited, Corning Community College (Corning CC), Finger Lakes Community College (Finger Lakes CC) and Monroe Community College (Monroe CC), are part of the State University of New York system and are sponsored by five counties (Chemung, Ontario, Monroe, Schuyler and Steuben) in western New York State. The Colleges each have a main campus and operate a total of 12 satellite locations, two extension centers and a field station. Between all campuses, the Colleges have approximately 6,000 computers. Total budgeted IT appropriations for the 2014-15 fiscal year were approximately $12.7 million.

The Colleges each have a computer network that stores student records and online resources (web applications) available to students via the Internet so they can register for classes, obtain grades, view transcripts, pay bills and update personal information, among other things. In total, the Colleges have 204 physical and virtual servers that provide support for the websites and web applications.

[1] Such as students, staff and faculty

Scope and Objectives

The objectives of our audit were to assess software management and website, web application and supporting server vulnerabilities for the period September 1, 2013 through April 30, 2015.[2] Our audit addressed the following related questions:

- Are College officials effectively and efficiently managing software licenses?
- Do security vulnerabilities exist in College websites, web applications or supporting servers?

Our audit examined the adequacy of certain IT controls. Because of the sensitivity of some of this information, we do not discuss certain results in this report, but instead communicated them confidentially to College officials.

Audit Results

College officials and IT staff can more effectively and efficiently manage software licenses. Two Colleges (Corning CC and Monroe CC) have not adopted adequate acceptable use policies that include practices for enforcement of the policy terms, such as monitoring computer use and reviewing installed software. Corning CC's policies also did not include penalties for noncompliance. Finger Lakes CC included provisions for enforcement in their policy, but did not develop supplemental procedures to detail how it plans to implement this aspect of the policy.

College officials and IT staff did not maintain a comprehensive inventory listing of purchased software or associated licenses[3] and did not routinely monitor or review computers for appropriateness of installed software. Corning CC and Finger Lakes CC had electronic tools available to generate reports of installed software, but did not effectively use these reports to monitor installed software. Through our review of selected computers, we found installations of nonbusiness and nonacademic related software on College computers such as gaming, instant messaging, golf management and couponing installations, as well as a virus. The installation of inappropriate or unlicensed software may be exposing College computers and networks to unnecessary risks, such as hacking or other malicious events.

Comments of College Officials

The results of our audit and recommendations have been discussed with College officials, and their comments, which appear in Appendix A, have been considered in preparing this report.

---

[2] Specific point-in-time testing for software installations was performed in December 2014 for Corning CC, January 2015 for Monroe CC and February 2015 for Finger Lakes CC. See Appendix B, Audit Methodology and Standards, for specific dates.

[3] However, upon our request for an inventory listing, staff from the Corning CC and Finger Lakes CC IT departments were able to provide us with records and documentation for software that would have been included on such an inventory.

Introduction

Background

Software assets have become increasingly important to local governments. Not only are they a vital element of information technology (IT) services that enable business-critical processes, but they also represent a large proportion of IT costs. Local governments also risk potential fines and penalties for using software applications that are not properly licensed. Additionally, local governments risk significant payroll overtime, consulting fees and equipment costs when unapproved or non-authentic software is installed on their networks, introducing unwanted, uninvited and often unintended consequences such as unforeseen crashes, breaches or system failures. Therefore, local governments need an understanding of the software they own, how it is used and how best to track user rights to ensure licensing compliance. Additionally, websites and related supporting servers are also an area of significance as attackers could identify vulnerabilities and use them to their advantage to gain unauthorized access to a network, possibly exposing a network or data to security threats. Strong website and related network security could result in decreased intrusions on a system and risks associated with data breaches.

Software management and website security are of particular importance to larger local governments, such as colleges, that have many different users[4] that perform a variety of functions. Typically, colleges will have several software applications and multiple licenses for each.

The three colleges we audited, Corning Community College (Corning CC), Finger Lakes Community College (Finger Lakes CC) and Monroe Community College (Monroe CC), are part of the State University of New York system and are sponsored by five counties (Chemung, Ontario, Monroe, Schuyler and Steuben) in western New York State. The Colleges are each governed by a Board of Trustees (Board), which is responsible for the general management and control of each College's financial and educational affairs. The Colleges each have a main campus and operate a total of 12 satellite locations, two extension centers and a field station. Between all campuses, the Colleges have approximately 6,000 computers. Total budgeted IT appropriations for the 2014-15 fiscal year were approximately $12.7 million.

The Colleges each have a computer network that stores student records and online resources (web applications) available to students

[4] Such as students, staff and faculty

via the Internet so they can register for classes, obtain grades, view transcripts, pay bills and update personal information, among other things. In total, the Colleges have 204 physical and virtual servers that provide support for the websites and web applications.

Objectives

The objectives of our audit were to assess software management and website, web application and supporting server vulnerabilities. Our audit addressed the following related questions:

- Are College officials effectively and efficiently managing software licenses?
- Do security vulnerabilities exist in College websites, web applications or supporting servers?

Scope and Methodology

We examined installed software and licenses on College computers and website, web application and supporting server vulnerabilities for the period September 1, 2013 through April 30, 2015.[5] We interviewed College officials and staff and reviewed policies and procedures related to IT to identify the controls established. We also reviewed 36 randomly selected[6] computers at each College to determine if the installed software was appropriate and if the Colleges had proper licenses and performed web vulnerability testing. Our audit also examined the adequacy of certain IT controls. Because of the sensitivity of some of this information, we did not discuss certain results in this report, but instead communicated them confidentially to College officials.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix B of this report.

Comments of College Officials

The results of our audit and recommendations have been discussed with College officials, and their comments, which appear in Appendix A, have been considered in preparing this report.

---

[5] Specific point-in-time testing for software installations was performed in December 2014 for Corning CC, January 2015 for Monroe CC and February 2015 for Finger Lakes CC. Website vulnerability testing was performed December 2014 through April 2015. See Appendix B, Audit Methodology and Standards, for specific dates.

[6] For each College, we obtained a hardware inventory listing of all College computers by location and user type. We selected a total of 36 computers for review based on the following categories: student-main campus (three computers), student-satellite locations (three computers), faculty/staff-main campus (25 computers) and faculty/staff-satellite locations (five computers).

Software Management

The management of software and licenses is essential to safeguarding College assets and data. Therefore, local governments need to have an understanding of the software they own, how it is used and how best to track user rights to ensure licensing compliance. The effective management of software also includes ensuring that only appropriate business or academic software is installed to reduce the risk of unwanted consequences that could result from unauthorized software. This can be done, in part, by establishing a strong acceptable use policy, limiting users' ability to install software, regularly reviewing computers to identify installed software and taking action to remove any unauthorized software.

College officials and IT staff can more effectively and efficiently manage software licenses. Corning CC and Monroe CC have not adopted adequate acceptable use policies that include practices for enforcement of the policy terms and Corning CC's policies did not include penalties for noncompliance. Finger Lakes CC included provisions for enforcement in its policy, but did not develop supplemental procedures to detail how it plans to implement this aspect of the policy. IT staff at all three Colleges also did not maintain a comprehensive inventory listing of purchased software or associated licenses. In addition, College officials and IT staff at all three Colleges did not routinely monitor or review computers. Finger Lakes CC did purchase a software auditing tool and implemented an informal practice of reviewing installed software on selected computers in February 2015. Through our review of computers at the Colleges, we found installations of nonbusiness and nonacademic related software on College computers such as gaming, instant messaging, golf management and couponing installations, as well as a virus.[7] The installation of inappropriate or unlicensed software may be exposing College computers and networks to unnecessary risk, such as hacking or other malicious events.

Acceptable Use Policy

Good controls over computerized data include an acceptable use policy that informs users about the proper use of College computers and requires the monitoring of computer usage to ensure compliance. An acceptable use policy defines the Board's goals for the use of equipment and computing systems and the security measures to protect the College's resources and confidential information. The policy should address, but not necessarily be limited to, the acceptable use

[7] Four installations at Corning CC, six installations at Monroe CC and one installation at Finger Lakes CC

of email accounts, Internet access and the installation of software on College computers. It is important that the policy provide provisions for enforcement and penalties for noncompliance and that system users provide written acknowledgement that they are aware of, and will abide by, the policy.

At each College, the Board adopted an acceptable use policy that outlines guidelines related to software installation and usage. However, at Corning CC and Monroe CC, these guidelines were limited because they did not detail practices for enforcement, such as monitoring computer use and reviewing installed software. In addition, Corning CC's policies did not include penalties for noncompliance. Although the Finger Lakes CC policy included provisions for IT department enforcement and monitoring, the IT department did not develop written procedures to formally detail how it planned to implement this aspect of the policy. Additionally, users at Corning CC and Monroe CC are not required to provide written acknowledgment that they will comply with the policy terms.[8] We also found that the policies at Monroe CC and Corning CC were not regularly reviewed and did not show any evidence of review or updating since at least 2011. The lack of an adequate acceptable use policy significantly increases the risk that hardware and software systems and the data they contain may be lost or damaged by inappropriate use. This leaves the Colleges vulnerable to risks associated with personal use, including computer viruses and spyware that could potentially be introduced by accessing nonbusiness or nonacademic related websites or downloading unauthorized software. In addition, enforcement of policy terms may be limited.

Software Inventory

The purpose of a software license is to grant an end user permission to use one or more copies of software in accordance with copyright law. When a software package is sold, it is generally accompanied by a license from the manufacturer that authorizes the purchaser to use a certain number of copies of the software. Local governments must obtain licenses commensurate with the number of copies in use. The implementation of a complete and comprehensive software inventory list is crucial to safeguard IT assets from potential unlicensed software being installed on computers. As a best practice, the list should include all College-owned software installed on computers, including software that does not require a purchased license, and the number of copies currently in use. Furthermore, the list should be used in regularly reviewing all computers owned by the Colleges to ensure that all software installed is properly approved and licensed.

[8] At Monroe CC, a screen with the summarized policy terms prompts each time a user attempts to log on to the network. Users are required to click "OK" prior to logging in to the network, but this does not ensure that users are aware of the full policy and all terms and expectations.

We found the Colleges' IT staff did not maintain a comprehensive inventory list of all software that each College owned or the total number of licenses for each software. However, the IT departments at Corning CC and Finger Lakes CC were able to provide records and documentation for software that would have been included on such an inventory list. At Monroe CC, individual departments are responsible for maintaining supporting documentation for software purchased and installed on department computers. The departments were able to provide IT staff with records and documentation for most of the software that would have been included on such an inventory list.[9]

In addition, none of the Colleges' IT staff performed regular audits of software installed on computers. Corning CC and Finger Lakes CC had electronic tools available to generate reports of installed software, but they did not effectively use these reports to monitor installed software. IT staff at the three Colleges also did not develop formal procedures for the regular review of individual computers or for removing nonbusiness related software installed on College computers. For Corning CC and Monroe CC, the regular review of computers is critical for reviewing installed software because these Colleges provide certain faculty and staff users with administrative rights. Therefore, users were able to download and install software without prior permission or approval. As a result, the IT staff may not be aware of all installed software.

Although there were no formal procedures for regular review, each of the Colleges' IT staff developed its own informal practice for reviewing installed software. The approaches were all different with varying levels of effectiveness. For example, Corning CC reviews a report of installed software annually, but does not remove inappropriate software when identified. Monroe CC reviews computers reported to have issues and removes inappropriate software identified,[10] and Finger Lakes CC implemented a new practice to review installed software on selected computers with the assistance of a software auditing tool.

Because IT staff did not maintain a comprehensive software inventory list or perform regular, formal reviews of College computers, there is an increased risk of unauthorized software being installed and not detected. Further, the lack of regular reviews of software installations, along with some users at two of the Colleges having administrative rights, resulted in nonbusiness or nonacademic related software being installed on certain computers.

---

[9] See Software Monitoring section for more information.

[10] Administrative rights will also be removed from computers in circumstances where repeated issues occur.

Software Monitoring

Each of the Colleges developed acceptable use policies to provide users with guidelines for IT asset use and security. Generally, the policies authorized use for college-related work and prohibited users from violating laws including copyright infringement.

To determine if installed software was authorized, had valid licenses (when required), was for a legitimate business purpose and was in compliance with the Colleges' acceptable use policies, we selected 36 computers[11] for review at each College. Overall, we identified approximately 2,610 software installations,[12] of which 220 required licensing. We requested purchase orders,[13] licenses and user agreements to verify that the Colleges had proper licensing to cover all copies of software installed on the computers reviewed. Corning CC and Finger Lakes CC were able to provide supporting documentation for all installed software programs that required licensing, all of which we also found to serve a legitimate business purpose. The Monroe CC departments could not provide purchase orders or other supporting documentation for two installed software programs that required licensing. We found these programs to serve a legitimate business purpose; however, without proper documentation, Monroe CC cannot ensure that the programs were properly licensed.

We found that all of the Colleges had at least one computer[14] used by a staff or faculty member with installed software that was not reasonable for academic or business purposes. The inappropriate software included gaming programs at Corning CC and Monroe CC, an instant messaging related program at Corning CC, coupon applications and a virus at Monroe CC and a golf management program at Finger Lakes CC. Based on the nature of these programs, they do not serve a legitimate work-related purpose and are in violation of the Colleges' acceptable use policies. Furthermore, non-College related programs may interfere with employees' work responsibilities.

Because certain users at two Colleges had administrative rights, thorough regular monitoring of College computers is not performed and two Colleges did not enforce their acceptable use policies, the installation of software that is not appropriate for a business or academic purpose was not identified or removed and violations of

[11] See Appendix B, Audit Methodology and Standards, for more information.

[12] A portion of these installations included upgrades and components of larger software programs.

[13] An effective and efficient method for purchasing and accounting for software licenses is through a purchase order system. A purchase order serves as the source document for vendor payment claims for various licenses obtained by the College and provides a record of licenses on hand to avoid duplicate purchases.

[14] Corning CC – four computers, Monroe CC – four computers and Finger Lakes CC – one computer

the Colleges' acceptable use policies went undetected. Potentially unauthorized software and software that doesn't serve a College business purpose may increase the risk that unauthorized access or modification to the computer system environment may occur, and the individual computer or network may be exposed to harmful events. In addition, because one of the Colleges' acceptable use policies did not require users to accept the terms or include penalties for noncompliance, enforcement of the policy's terms may be limited.

Recommendations

College officials should work with IT staff to:

1. Update their acceptable use policy to include specific guidance related to software downloads and installations, as well as enforcement and penalties for noncompliance. This policy should be regularly reviewed, updated and distributed to users to obtain their written agreement of compliance with the policy terms.

2. Ensure that administrative rights are limited to only those College employees with a need for such access.

3. Maintain a complete, comprehensive software inventory list of all software that the College owns and the total number of licenses for each software.

4. Formalize procedures to perform reviews of software installed on College computers and compare results to the College's software inventory list.

5. Monitor users to ensure compliance with the acceptable use policy and ensure software installed on College computers is business and/or academic appropriate.

APPENDIX A

RESPONSES FROM COLLEGE OFFICIALS

We provided a draft copy of this global report to each of the Colleges we audited and provided each College with an opportunity to respond to the global report. We received response letters from all three of the Colleges. College officials generally agreed with our findings and recommendations and indicated that they intend to implement corrective action. The following comments were excerpted from the responses we received. Comments that were specific to findings at a particular College are not included here, but are instead addressed in the College's individual letter report. Our findings at each of the three Colleges, and each College's response to our findings, are contained in the individual letter report addressed to each College.

Corning Community College

"As internet and cloud technologies are evolving into what is now referred to as the 'Internet of Things,' the OSC's findings are instrumental in further developing and strengthening Corning CC's digital safeguards for our students, employees, and campus visitors. Acting upon the recommendations of the OSC Audit will enable Corning CC to continue, in an enhanced fashion, to ensure the safety and viability of the digital information entrusted to us, including such critical and personal information as grades and financial records."

Finger Lakes Community College

"With these corrections implemented (as submitted by the Chief Information Officer), Mr. Taylor confirms that we will agree with the findings and feels that the recommendations made are appropriate." "The Finger Lakes Community College Board of Trustees Audit and Enterprise Risk Management Committee has also reviewed a summary of the findings and process going forward, and is in agreement with all."

Monroe Community College

"We believe these recommendations will help to improve the Information Security and Technology operations within the College." "MCC is committed to a safe and secure computing environment and will address the recommendations of the audit."

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

The objectives of our audit were to determine if College officials efficiently and effectively managed software licenses and whether security vulnerabilities exist in College websites, web applications or supporting servers. To achieve the objectives of this audit and obtain valid audit evidence, we performed the following audit procedures:

- We selected three community colleges within the region that had not been recently audited by our Office: Corning CC, Finger Lakes CC and Monroe CC.

- We interviewed College officials and staff and reviewed IT policies and procedures to determine the internal controls in place.

- For each of the Colleges, we obtained a computer inventory list for all campuses from IT staff and sorted this list by location and end user (i.e., students, faculty and staff). From the inventory lists, we randomly selected 36 College-owned computers for review: 25 faculty/staff and three student computers were selected at the main campus, and five faculty/staff and three student computers were selected at the satellite campuses. We used specialized audit software to obtain a list of all software installed on each machine. We reviewed the installations for licensing requirements and to determine if they served a legitimate business purpose.

    - For Corning CC – Specific point-in-time testing for software installations was performed on December 4, 8, 9 and 15, 2014. Website vulnerability testing was performed over the period December 2014 through January 2015.

    - For Finger Lakes CC – Specific point-in-time testing for software installations was performed on February 25 and 26, 2015. Web vulnerability testing was performed over the period of March through April 2015.

    - For Monroe CC – Specific point-in-time testing for software installations was performed on January 13, 14 and 15, 2015 and February 9, 2015. Web vulnerability testing was performed over the period of January through March 2015.

- We reviewed the provided license agreements and purchase orders to determine if the Colleges authorized all software and whether the Colleges maintained licensing for the software installed on each of the computers reviewed.

- We reviewed the Colleges' websites and performed vulnerability testing on College websites, web applications and supporting servers using specialized scanners and audit tools.

We conducted this performance audit in accordance with 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX D

OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE
Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington Counties

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608
(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

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence Counties

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313