DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2017M-213

Columbia-Greene Community College

Information Technology

DECEMBER 2017

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights 1

Information Technology 2

What Are Effective Information Technology Controls? 2

The Board Did Not Adopt Procedures for Managing System Access . 2

The Board Did Not Adopt a Breach Notification Policy 2

Internet Usage Was Not Routinely Monitored 3

The Disaster Recovery Plan Has Not Been Tested 3

The College Does Not Provide Adequate Cybersecurity Training to Employees 3

What Do We Recommend? 4

Appendix A: Response From College Officials 5

Appendix B: Audit Methodology and Standards 8

Appendix C: Resources and Services 9

Report Highlights

Columbia-Greene Community College

Audit Objective

To determine if College officials ensured that the College's Information Technology (IT) system was adequately secured and protected against unauthorized use, access and loss.

Key Findings

- The College has 2,498 user accounts that have not been used in the last six months, with the oldest employee account's last logon being over 10 years ago.
- The College did not adopt a breach notification policy.
- Five employees visited music streaming, social media and shopping websites which could expose the network to virus attacks or compromise systems and data.
- The College has never tested its disaster recovery plan; therefore, information may not be adequately safeguarded.

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

Key Recommendations

- Adopt procedures for managing system access and a breach notification policy.
- Review the Internet usage log to ensure compliance with the College's computer use policy.
- Test the disaster recovery plan.
- Address the IT recommendations communicated confidentially.

College officials agreed with our recommendations and indicated they planned to initiate corrective action.

Background

The Columbia-Greene Community College (College) is located in the Town of Greenport in Columbia County. The College is governed by a Board of Trustees (Board), which is composed of 10 members. The Board is responsible for the general management and control of the College's financial and educational affairs. The President of the College is the chief executive officer and is responsible for the College's administration. The Dean of Administration is the chief fiscal officer. The IT Director is the network administrator, responsible for hardware application acquisitions or changes and for monitoring service agreements.

Quick Facts

Approximate Number of Employees	560
Approximate Number of Computers	525

Audit Period

September 1, 2015 – July 31, 2017

Information Technology

The College's IT system and data are valuable resources. The College relies on its IT system for Internet access, email and for maintaining financial, personnel and student records. If the IT system is compromised, the results could range from inconvenient to catastrophic and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

What Are Effective Information Technology Controls?

College officials should develop comprehensive written procedures for managing system access that include periodic reviews of user access to ensure that user accounts are disabled or deleted when access is no longer needed. In addition, New York State (NYS) Technology Law requires local governments to adopt a breach notification policy that establishes how officials would notify affected parties whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. A computer use policy should be adopted that describes appropriate and inappropriate use of IT resources and compliance with that policy should be monitored by IT officials. Also, a disaster recovery plan should be adopted to anticipate and plan for an IT disruption involving the corruption or loss of data and the plan should be tested to ensure that employees understand their roles and responsibilities in a disaster situation. Finally, cybersecurity training should be provided to employees at least annually to address current risks identified by the IT community such as computer use, phishing and social media.

The Board Did Not Adopt Procedures for Managing System Access

The Board has not adopted comprehensive written procedures for managing system access. Consequently, the College's Active Directory database has 2,317 student accounts and 181 employee accounts that have not been not used in the last six months. The oldest employee account had a last logon of May 22, 2007, over 10 years ago. Having inactive user accounts increases the Active Directory's attack surface. Additionally, because these user accounts are inactive, they are most likely not monitored, making it unlikely that staff would notice these accounts being compromised or used for malicious purposes.

The Board Did Not Adopt a Breach Notification Policy

The IT Director has a breach notification policy in a draft format, but it has never been approved by the Board. Without a formal breach notification policy, officials and employees may not understand or fulfill their legal obligation to notify affected

parties if private information is compromised putting them at risk of losing financial or personal data.

Internet Usage Was Not Routinely Monitored

The Board has adopted a computer use policy. However, the Internet usage log is not routinely reviewed for compliance with that policy. We tested five employees' web histories and determined they were not complying with the policy. All five employees visited music streaming, social media, personal email, sports, shopping, travel and entertainment websites which are against College computer use policy. Additionally three employee computers contained a large amount of advertising content, which could indicate adware.[1] The inappropriate use of the College's computers could expose the network to virus attacks or compromise systems and data, including key financial and confidential information. Furthermore, time spent by employees surfing the web for personal reasons while they are supposed to be working represents lost resources.

The Disaster Recovery Plan Has Not Been Tested

Although the College has a disaster recovery plan that appears adequate, it has never been tested to ensure that employees understand their roles and responsibilities in a disaster. The IT Director told us that to properly test the plan, a backup server would need to be used; however, the College does not have one readily available for this purpose. Without testing the plan, there is no assurance that information will be safeguarded in the event a failure happens within the network.

The College Does Not Provide Adequate Cybersecurity Training to Employees

While the College provides brief IT training upon hire, there is no formal IT training on a regular basis. It is important to provide training to employees and to update the training material periodically to address current risks such as computer use, phishing and or social media. The IT Director has reviewed some training materials that he believes would be effective training, but has not sought Board approval for such training. Not providing cybersecurity training to employees increases the risk that users will not understand their responsibilities, putting the data and computer resources at greater risk for unauthorized access, misuse or abuse.

1 Adware automatically displays or downloads advertising material.

What Do We Recommend?

The Board should:

1. Adopt written procedures for managing system access that include periodically reviewing user access and disabling or deleting user accounts when access is no longer needed.

2. Adopt a breach notification policy in accordance with NYS Technology Law.

The IT Director should:

3. Review the Internet usage log to ensure compliance with the College's computer use policy.

4. Test the disaster recovery plan.

5. Ensure that cybersecurity training is provided periodically to all employees to address current risks as computer use, phishing and social media.

Appendix A: Response From College Officials

COLUMBIA GREENE COMMUNITY COLLEGE

4400 ROUTE 23
HUDSON, NY 12534
518-828-4181
518-828-8543 (FAX)
WWW.SUNYCGCC.EDU

December 13, 2017

Tenneh Blamah, Chief Examiner
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725

Dear Ms. Blamah,

Please accept this letter as the official response and corrective action plan to the Columbia-Greene Community College Information Technology report of examination 2017M-213.

We want to thank the examiners for the important work they do, and the College agrees with the recommendations outlined in the audit. The corrective action plan is as follows:

Unit Name: Columbia-Greene Community College
Audit Report Title: Information Technology
Audit Report Number: 2017M-213

For each recommendation included in the audit report, the following is our corrective action(s) taken or proposed. For recommendations where corrective action has not been taken or proposed, we have included the following explanations:

Audit Recommendation:

The Board Should:

1. Adopt written procedures for managing system access that include periodically reviewing user access and disabling or deleting user accounts when access is no longer needed.

2. Adopt a breach notification policy in accordance with NYS Technology Law.

The IT Director Should:

3. Review the Internet usage log to ensure compliance with the College's computer use policy.

4. Test the disaster recovery plan.

5. Ensure that cybersecurity training is provided periodically to all employees to address current risks as computer use, phishing and social media.

COLUMBIA GREENE COMMUNITY COLLEGE

4400 ROUTE 23
HUDSON, NY 12534
518-828-4181
518-828-8543 (FAX)
WWW.SUNYCGCC.EDU

Implementation Plan of Action(s):

1. We agree with the recommendation and will author written procedures for managing and periodically reviewing user access and disabling or deleting user accounts when access is no longer needed.

2. We agree with the recommendation and the College will adopt a breach notification policy.

3. We agree with the recommendation and the IT Director in cooperation with senior management will review logs for compliance with the College's computer use policy.

4. We agree with the recommendation and the CIS director will test the disaster recovery scenarios outlined in the Network disaster recovery plan.

5. We agree with the recommendation and the College will implement cyber security training for all employees.

Implementation Date:

1. 3/31/2018

2. 3/31/2018

3. 6/30/2018

4. 12/31/2018

5. 12/31/2018

Person Responsible for Implementation:

1. President, Director of CIS

2. President, Director of CIS

3. Director of CIS, Senior Management

4. Director of CIS

5. Director of CIS

COLUMBIA GREENE COMMUNITY COLLEGE

4400 ROUTE 23
HUDSON, NY 12534
518-828-4181
518-828-8543 (FAX)
WWW.SUNYCGCC.EDU

Signed:

Name
President

12/14/17
Date

Sincerely,

J.R. Campion, President

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 interviewed College officials and employees to obtain an understanding of the College's IT operations.
- We reviewed College records for any IT related policies and procedures and reviewed those policies and procedures to obtain an understanding of the College's IT operations.
- We judgmentally selected five of the eight computers in the Business Office based on the users' access to business applications and financial data. We analyzed the web browsing histories to determine whether employees were complying with the College's computer use policy.

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 College 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.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. We encourage the Board to make the CAP available for public review in the Clerk's office.

Appendix C: Resources and Services

Regional Office Directory
http://www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
http://www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
http://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
http://www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
http://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
http://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
http://www.osc.state.ny.us/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
http://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
http://www.osc.state.ny.us/localgov/training/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

Local Government and School Accountability Help Line: (866) 321-8503

NEWBURGH REGIONAL OFFICE – Tenneh Blamah, 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.state.ny.us

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

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