You're viewing an archived copy from the New Jersey State Library.

New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor

New Jersey Public Colleges' and Universities' Data Security

March 28, 2011 to July 31, 2011

Stephen M. Eells
State Auditor

You're viewing an archived copy from the New Jersey State Library.

2008 - 2009

LEGISLATIVE SERVICES COMMISSION

ASSEMBLYMAN
JOSEPH J. ROBERTS, JR.
Chairman

SENATOR
THOMAS H. KEAN, JR.
Vice-Chairman

SENATE

ANDREW R. CIESLA
RICHARD J. CODEY
NIA H. GILL
ROBERT M. GORDON
SEAN T. KEAN
JOSEPH M. KYRILLOS, JR.
LORETTA WEINBERG

GENERAL ASSEMBLY

PETER J. BIONDI
JON M. BRAMNICK
JOHN J. BURZICHELLI
ALEX DECROCE
ALISON LITTELL MCHOSE
JOAN M. QUIGLEY
BONNIE WATSON COLEMAN

New Jersey State Legislature

OFFICE OF LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR
125 SOUTH WARREN STREET
PO BOX 067
TRENTON NJ 08625-0067

ALBERT PORRONI
Executive Director
(609) 292-4625

OFFICE OF THE STATE AUDITOR
(609) 292-3700
FAX (609) 633-0834

STEPHEN M. EELLS
State Auditor

THOMAS R. MESEROLL
Assistant State Auditor

JOHN J. TERMYNA
Assistant State Auditor

The Honorable Chris Christie
Governor of New Jersey

The Honorable Stephen M. Sweeney
President of the Senate

The Honorable Sheila Y. Oliver
Speaker of the General Assembly

Mr. Albert Porroni
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the New Jersey Public Colleges' and Universities' Data Security for the period of March 28, 2011 to July 31, 2011. If you would like a personal briefing, please call me at (609) 292-3700.

Stephen M. Eells
State Auditor
February 28, 2012

You're viewing an archived copy from the New Jersey State Library.

Table of Contents

You're viewing an archived copy from the New Jersey State Library.

Scope

We reviewed the adequacy of security measures in place to protect information collected by New Jersey's public colleges and universities for the period March 28, 2011 to July 31, 2011. Excluded from the scope of this review were the state's three research universities: the New Jersey Institute of Technology; Rutgers, The State University of New Jersey; and the University of Medicine and Dentistry of New Jersey. We selected five of the nine public colleges and universities for evaluation of selected controls in place over the network and systems that process and protect both public and private information from unauthorized access. The review focused on the following areas.

- Administration and security over Internet-facing devices
- Website integrity
- Security over publicly-accessible wireless signals
- Physical security and environmental controls
- Asset tracking and disposal

The institutions selected were Thomas Edison State College, Rowan University, The Richard Stockton College of New Jersey, New Jersey City University, and Montclair State University. Excluded were The College of New Jersey, William Paterson University, Kean University, and Ramapo University. As such, we cannot attest to the particular issues at the colleges not selected for testing.

Objectives

The objective of our audit was to determine the adequacy of security measures in place to protect personally identifiable and confidential information collected by New Jersey's public colleges and universities. This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section I, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with *Governmental Auditing Standards* issued by the Comptroller General of the United States. Additional guidance for the conduct of the audit was obtained from the Open Source Security Testing Methodology Manual issued by the Institute for Security and Open Methodologies, the Federal Information System Control and Audit Manual (FISCAM), Control Objectives for Information and Related Technology (COBIT) issued by the IT Governance Institute, and other industry-wide information technology security resources.

You're viewing an archived copy from the New Jersey State Library.

In preparation for our testing, we studied legislation, vulnerability research, and industry and governmental standards for computer security and operation. Provisions that we considered significant were documented and compliance with those requirements was verified by interview of key personnel, observation and access of network infrastructure, and through other tests we considered necessary to validate a potential issue or its impact.

Preliminary evaluations of all nine non-research colleges were performed. Based on the potential risks identified as a result of those evaluations, we selected five of the nine public colleges and assessed a sample of their Internet-facing devices, public website integrity, wireless security, physical security and environmental controls, asset tracking and disposal, and other selected controls that contribute to the protection of data assets. The sample of institutions taken was to determine issues at each of the selected colleges and to draw conclusions about areas of improvement that were common to the institutions. A nonstatistical sampling approach was used. Our samples were designed to provide conclusions about internal control attributes. Sample items were selected judgmentally.

Conclusions

We found that each of the college and university IT staffs take securing their infrastructure seriously and that, generally, controls over data security were adequate. However, there were control areas where improvements could be made to make them more secure. Most critically, we discovered an instance where personally identifiable information was publicly accessible at one college. This situation was addressed by the college and remedied immediately. There were other issues that existed at multiple colleges that are addressed in this report and in each college's management letter.

You're viewing an archived copy from the New Jersey State Library.

Issues Reported Under Separate Cover

There were issues of a sensitive and technical nature that were common to the colleges and were reported in detail in each of the institution's management letters. In summary, the audit found issues in the following general categories: publicly accessible hosts, unnecessary ports and services enabled, unpatched or unsupported software, insecure coding, improper disclosure of information, broken or misdirected links, secure socket layer weaknesses, and website configuration issues. With the exception of the item noted in the conclusion, we found no instance of a vulnerability that revealed personally identifiable information, nor did we find any evidence that a server had been compromised by an attacker during the audit period. In addition, there were issues that existed at a single college and are only addressed in that particular college's management letter.

Wireless Security

The universities' wireless signals are not configured securely.

Each of the five colleges we visited provided a wireless signal for students or guests to use while on the institution's property. All of the colleges use an authentication system to control access to their wireless signals that requires the user to first connect to the signal using their wireless device, then authenticate before using any of the resources on the college network. At two of the colleges, we found that we could access some internal resources of the network prior to authentication. In addition, at one college we could scan external hosts as an unauthenticated user.

Industry standards require that remote wireless access be properly controlled to protect unauthorized access to sensitive system resources. From our discussions with the IT staff at the affected colleges we found that, with one exception, the colleges were not aware of these abilities of unauthenticated users. In each case, an improper configuration of a device in the wireless network was to blame. The colleges have begun correcting the issue, although one is using a consultant to upgrade their wireless network and must wait for the consultant to correct the issue. Because of the nature of public wireless networks, the signal must be broadcast over a wide area, which means that anyone can connect to it who is within range. The ability to connect to internal resources could pose a threat to the internal network, and the ability to connect to external hosts on the Internet could allow the colleges' signals to be used to launch an attack on a third-party device.

Recommendation

We recommend that the colleges continue their efforts to correct the improper configurations in order to restrict unauthenticated users from reaching any resources, either internal or external.

You're viewing an archived copy from the New Jersey State Library.

Asset Tracking and Disposal

The colleges need to improve the tracking and salvaging of computer equipment to ensure that all devices are properly sanitized during the decommissioning process.

Industry standards require that an organization have appropriate equipment, techniques, and procedures implemented to clear sensitive data from digital media before its disposal or release outside the organization. Those procedures should include the ability to accurately track a device throughout its life to ensure that proper disposal can be verified, as well as proper physical controls over media devices like hard drives to ensure that they are protected from loss prior to data sanitization.

We found issues in three of the five colleges we reviewed with regard to this process. One college had no asset tracking system in place to ensure that all devices were transferred to their third-party disposal company for data sanitization. Two colleges had not yet implemented a replacement tracking system for IT assets that are no longer tracked because dollar amount thresholds were raised. Although some of the machines currently in use still had tags on them from the previous system because of their purchase date, there is an increasing number of untagged machines in use not meeting the new dollar thresholds. These colleges were looking into addressing the issue. In addition, we found one college where unsanitized hard drives were left unsecured in a public area. Without proper controls to track these assets, there is an increased risk that a device containing personally identifiable or confidential information could be removed from the college without proper data sanitization.

Recommendation

We recommend that the colleges develop a method to ensure that all computer assets are tracked throughout their life cycle to ensure they are properly sanitized during the disposal process, and that all media containing data are properly stored and secured during the disposal process.

»➤◄«

Encryption Strategy

The colleges lack an encryption strategy for laptop computers assigned to faculty and staff.

Our review found that four of the five colleges did not employ an encryption strategy for laptops assigned to faculty and staff. Industry standards recommend that encryption procedures be implemented where appropriate based on risk. Since laptops are mobile, they are at a greater risk for theft or loss and should be encrypted to prevent data from being extracted in the event that a loss occurs.

You're viewing an archived copy from the New Jersey State Library.

The four colleges without encryption expressed that they had considered encryption for these devices and were in the process of evaluating different products, though none had implemented a strategy during the review period.

Recommendation

We recommend that the colleges implement an encryption strategy on all faculty and staff laptops to protect data contained on them in case of a loss.

Physical and Environmental Controls

Issues with environmental controls could put the IT assets of the colleges at risk.

Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. Physical controls also include environmental controls such as smoke detectors, fire alarms and extinguishers, and power supplies. We conducted reviews of the main and backup computer facilities and a sample of other areas housing IT assets for select physical and environmental controls, including a "red light" test of devices to determine if there were any potential equipment failures.

We found that four of the five colleges reviewed had issues with environmental controls in their computer facilities. Three colleges had no smoke or water detectors and one had no fire extinguishers in their data centers. In addition, one college had two devices running in the data center with issues. One was in failover mode, the other had a failed drive.

A lack of proper environmental controls like these could put computer facilities at an increased risk for damage from smoke, fire, or water that could be greatly reduced by detection systems or extinguishers. Also, periodic reviews of equipment for failures or issues could help avoid downtime caused by device failure.

Recommendation

We recommend that the colleges institute the missing environmental controls in their computer facilities, as well as conduct periodic reviews of devices in the computer room to look for warning lights or other signs of potential problems with devices.

You're viewing an archived copy from the New Jersey State Library.

Configuration Management

Failure to baseline the initial configuration of devices could allow authorized or unauthorized changes to be made without detection.

Industry standards recommend that an entity maintain current configuration information baselines on devices in their network. These consist of the initial configuration baseline, plus all approved changes to the initial configuration. Two of the colleges we reviewed do not baseline their initial operating systems and software installation, therefore they may be unable to determine if a change had occurred to the configuration. The other three colleges not only established baselines, but two were employing tools to monitor for unauthorized configuration changes on a continual basis.

Failure to record baseline initial configurations means that the colleges may be unaware of unauthorized changes that may have taken place, and therefore may have current configurations that differ from what the college would expect.

Recommendation

We recommend that the colleges establish an initial configuration for devices, and update and monitor those configurations as needed to prevent unauthorized changes.

Policies and Procedures

Internal policies and procedures are not written, formalized, and/or up to date.

Entities should, as part of a comprehensive plan for addressing security, document and approve security policies and procedures for their organization. The policies should be adequate to address the risks identified by the entity and should be updated periodically to reflect changes. Our review at the five colleges found that four had issues regarding formal written policies and procedures. One college did not have a policy on the handling of security incidents. Another college did not have internal operating procedures for their IT unit. Two of the colleges had policies and procedures that either were in draft form or had not been revised since 2005. Changes in technology require policies and procedures to be reviewed and reapproved on a regular basis to adapt for these changes. All the colleges are working toward resolving the issues based on our work.

Recommendation

We recommend that the colleges create and approve formal IT policies and procedures, and review and revise them on a regular basis.

You're viewing an archived copy from the New Jersey State Library.

Summary of Auditee Responses

In order to not identify any college or university specifically on the corrective action taken on our audit recommendations, we have summarized their responses, by finding, below.

Items Reported Under Separate Cover

In summary, the audit found issues in the following general categories: publicly accessible hosts, unnecessary ports and services enabled, unpatched or unsupported software, insecure coding, improper disclosure of information, broken or misdirected links, secure socket layer weaknesses, and website configuration issues. With the exception of one item noted in the conclusion, we found no instance of a vulnerability that revealed personally identifiable information, nor did we find any evidence that a server had been compromised by an attacker during the audit period.

Response:

The colleges reported that where necessary, servers have either been retired or replaced. Additionally, unnecessary ports and services have been disabled, more secure protocols have been implemented where possible, website configurations issues have been corrected or recommended to the group(s) that maintain the application, and unpatched and unsupported software has been patched or upgraded to supported versions. Other issues noted have been corrected with other solutions being researched prior to being implemented.

Wireless Security

At two of the five colleges, we found that we could access some internal resources of the network prior to authentication. In addition, at one college we could scan external hosts as an unauthenticated user.

Response:

The colleges and universities affected have indicated that steps have been taken to block this type of access. Vendors and consultants currently under contract for design and implementation of wireless infrastructure were advised of the issues noted in the public report and have been requested to look into and correct any deficiencies noted.

Asset Tracking and Disposal

At three of the five colleges reviewed, one had no asset tracking system in place to ensure that all devices were transferred to their third-party disposal company for sanitization, while two had not yet implemented a replacement tracking system for IT assets no longer tracked because the dollar amount thresholds were raised. Also, at one college hard drives that were reused were not properly sanitized for redeployment.

You're viewing an archived copy from the New Jersey State Library.

Response:

The colleges responded that steps have been taken to destroy all decommissioned hard drives and install new ones in redeployed workstations. With regard to the asset tracking systems, the colleges affected indicated that steps have been taken to begin accounting for PC related assets purchased through the IT office and have communicated with senior management the importance of this function.

Encryption Strategy

Four of the five colleges did not employ an encryption strategy for laptops assigned to faculty and staff.

Response:

The colleges responded that all newly purchased laptops issued to faculty and staff will have some type of encryption on them. For one college, encryption standards for portable storage devices are currently being developed.

Physical and Environmental Controls

Four of the five colleges reviewed had issues with environmental controls in their computer facilities. Three colleges had no smoke or water detectors and one had no fire extinguishers in their data centers. In addition, one college had two devices running in the data center with issues. One was in failover mode, the other had a failed drive.

Response:

The colleges affected indicated that steps have been taken to install fire extinguishers in their data centers and install smoke and water detectors where necessary. The issues noted on the two devices have been mitigated.

Configuration Management

Two of the five colleges reviewed do not baseline their initial operating systems and software installation, therefore they may be unable to determine if a change has occurred to the configuration. The other three colleges not only established baselines, but two were employing tools to monitor for unauthorized configuration changes on a continual basis.

Response:

The colleges responded that they have been researching solutions. Once one is selected, it will be tested and implemented.

You're viewing an archived copy from the New Jersey State Library.

Policies and Procedures

Our review at the five colleges found that four had issues regarding formal written policies and procedures. One college did not have a policy on the handling of security incidents. Another college did not have internal operating procedures for their IT unit. Two of the colleges had policies and procedures that either were in draft form or had not been revised since 2005.

Response:

The colleges responded that they are currently in the process of documenting their policies and procedures and are reviewing and updating them where necessary.