An Audit Report on

Protection of Confidential Data and Critical Information Systems at Texas A&M University

September 2004

Report No. 05-003

State Auditor's Office

Lawrence F. Alwin, CPA
State Auditor

An Audit Report on

Protection of Confidential Data and Critical Information Systems at Texas A&M University

SAO Report No. 05-003
September 2004

Overall Conclusion

Although Texas A&M University (University) has established generally adequate controls to protect confidential data and critical information systems from loss or unauthorized access and use, it does not consistently apply these controls, and other information system controls are not functioning as intended. We identified specific weaknesses in access controls for certain data and applications (see text box); noncompliance with information technology policies, legal requirements, and University procedures; and weaknesses in disaster recovery planning.

Background Information

Our audit focused on the Student Information Management System (SIMS) and the Financial Accounting Management Information System (FAMIS). These systems contain confidential information on the University's 44,800 students and 8,600 faculty and staff, such as:

- Social Security numbers.
- Students' grades.
- Students' financial information.
- Information on students' parents.

Key Points

The University should tighten controls over access to computer resources to reduce the risk that confidential data could be exposed to loss or unauthorized access and use.

The University should improve its periodic reviews of users' access to critical applications to better ensure that users have only the access they need and that terminated employees' access is promptly canceled. It should also strengthen and better enforce password policies and improve security over network access and file transmissions to prevent unauthorized access to data. In addition, the University should address specific access weaknesses that could allow programmers to make unauthorized changes to applications. However, the University has implemented a generally strong wireless access program and a properly configured firewall, both of which help to protect its data from unauthorized access.

The University should improve its compliance with information technology policies, legal requirements, and University procedures to ensure that its efforts to protect data and computer resources are not undermined.

The University needs to fully implement, on a University-wide basis, 16 of the 22 information security policies required by the Texas Administrative Code (TAC), and campus departments need to provide required security awareness training to their network users. However, the University has developed a good methodology for performing the risk assessment required by the TAC and the federal Gramm-Leach-Bliley Act.

State Auditor's Office
Lawrence F. Alwin, CPA
State Auditor

This audit was conducted in accordance with Texas Government Code, Sections 321.0131 and 321.0132.

For more information regarding this report, please contact Ron Franke, Audit Manager, at (512) 936-9500.

The University should improve its disaster recovery plan and related procedures for critical data and applications to ensure that it is able to restore computer resource capabilities promptly in the event of a disaster.

The University should better protect its backup tapes of critical data from the risk of fire. It also should develop procedures for required periodic updating of its disaster recovery plan for critical data and applications and develop a plan for conducting required annual testing of that plan.

Summary of Information Technology Review

We focused on the security of confidential data in student and financial systems, as well as the University's management of central information resources. We conducted technical vulnerability scans and wireless leakage tests in selected areas, but we did not attempt to exploit the vulnerabilities we identified. We did not review controls over the Texas A&M University System's Budget/Personnel/Payroll System or other systems that are unrelated to the student or financial systems.

Summary of Management's Response

Management generally agrees with our recommendations and is taking action to address our findings.

Summary of Objective, Scope, and Methodology

The objective of this audit was to determine whether the University has adequate controls to protect confidential data and critical systems from loss or unauthorized access and use.

Our audit scope included general controls over all of the University's information systems and application controls for the University's student and financial systems as of May 2004.

Our methodology included interviewing staff, reviewing disaster recovery and information security plans and policies, inspecting major data centers, and conducting network and wireless scans to identify potential information systems vulnerabilities.

Table of Results and Recommendations

The University does not always ensure that users' access to applications is necessary. (Page 3)

The University should:

- Ensure that all users of critical applications are current employees whose job duties require access to those applications.
- Require departments responsible for SIMS data to identify key confidential data and regularly review users' access to this data.
- Change the mainframe authentication rule to revoke inactive user accounts after a specified period of inactivity.
- Review all applications and domains to identify user accounts that have never been used or that have not been used within a reasonable period of time (for example, within the past four months) and determine whether these accounts should remain active.

Weaknesses in password policies and in the enforcement of password policies could impair data security. (Page 6)

The University should:

- Enforce all password policies and ensure that the policies require that:
    - All accounts on servers have passwords.
    - Passwords be at least six characters long.
    - To the extent possible, passwords include a combination of uppercase and lowercase letters, numbers, and special characters.
    - Passwords differ from the user names on the accounts.
    - Passwords expire after 90 days.
- Determine an acceptable period of time for passwords to be maintained in history to prevent their reuse, and include this requirement for all accounts.

The University does not always ensure that changes to applications are properly authorized and documented. (Page 7)

The University should set up security in its change management software to require a second-level review of all SIMS code changes.

The Texas A&M University System should continue its plans to implement automated change-tracking software for FAMIS.

The University does not always ensure that internal access to data is appropriately secured. (Page 8)

The University should:

- Disable TelNet and FTP and implement a secure, encrypted method of access to SIMS.
- Review its server-patching process and determine what improvements can be made to keep systems patched.
- Verify that servers are configured correctly to eliminate unnecessary login accounts.
- Verify that services running on servers are necessary and either (1) patch and configure these services securely or (2) disable these services.
- Activate the account lockout feature on all servers and configure it to deactivate accounts after repeated unsuccessful login attempts.

The University does not always ensure that external access to its main network and data through wireless devices is appropriately secured. (Page 10)

The University should:

- Frequently scan to identify unauthorized wireless access points in University-occupied buildings (on and off campus) and take appropriate action to remove these access points or ensure that the security of these access points is adequate.
- Activate the account lockout feature on its wireless authentication server and configure it to deactivate accounts after repeated unsuccessful login attempts.

Table of Results and Recommendations

External scans of the University's computer network identified no vulnerabilities. (Page 11)

(No recommendations)

The University should ensure compliance with required policies, legal requirements, and University policies and procedures. (Page 12)

The University should:

- Fully implement all security policies required by the TAC on a University-wide basis. If responsibility for implementing these policies is left with the individual campus departments, the University should perform monitoring of the departments to ensure that the required policies have been implemented.
- Ensure that all network users attend security awareness training on an ongoing basis. This could be done by a mandate from executive management or by delegating this responsibility to the departments and regularly monitoring the departments' progress.

The University should strengthen disaster recovery plan processes and procedures for critical data and applications. (Page 14)

The University should:

- Protect backup tapes of critical data from fire damage by storing them in a fireproof container or installing a fire suppression system in the storage room.
- Develop a plan for testing its disaster recovery plan for critical data and applications and test the plan at least annually, particularly for its most critical systems.
- Develop written procedures for reviewing and revising the disaster recovery plan for critical data and applications.

Recent SAO Work

Number	Product Name	Release Date
04-009	A Financial Review of Prairie View A&M University	November 2003

Contents

Detailed Results

Appendix

Detailed Results

Introduction

Texas A&M University (University) collects and stores a significant amount of confidential data in automated systems. For example, the University collects personally identifiable information for its 44,800 students, such as Social Security numbers, grades, medical information, financial information, and information about students' parents. It also collects personally identifiable information for its 8,600 faculty and staff members.

Federal Laws Requiring Protection of Information

The Family Educational Rights and Privacy Act (FERPA; 20 U.S.C. Section 1232[g], 34 CFR Part 99) is a federal law that protects the privacy of student education records. Generally, schools must have written permission from a parent or eligible student in order to release any information from the student's education record except for "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance.

The Safeguards Rule of the Gramm-Leach-Bliley Act (GLB Act; 15 U.S.C. Section 6801-6809, 16 CFR Part 314) establishes standards for financial institutions to ensure the security and confidentiality of customer records and information. Although the GLB Act was geared toward financial institutions, the U.S. Federal Trade Commission has determined that the Act also applies to colleges and universities because they provide loans to students.

It is critical that the University protect this data because:

- Federal laws such as the Family Educational Rights and Privacy Act and the Gramm-Leach-Bliley Act require the University to safeguard certain data (see text box).
- Unauthorized disclosure of confidential data could lead to civil lawsuits from individuals who suffer damages.
- The University's reputation could be harmed as a result of the unauthorized disclosure of or failure to limit access to confidential data.
- The increase in cases of identify theft highlight the need for better protection of confidential data. The U.S. Federal Trade Commission reports that more than 200,000 individuals (including 20,634 Texans) were the victims of identify theft in 2003.[1]

Recent events both in Texas and in other parts of the country demonstrate why it is critical for the University to properly safeguard data:

- In 2003, officials at Southern University in Baton Rouge, Louisiana, discovered that 541 past and current students had paid an employee of this institution to change their grades. This had occurred without detection for a period of nine years.[2]
- In 2003, The University of Texas at Austin learned that a hacker had gained access to one of its databases and had stolen approximately 55,000 Social Security numbers.[3]

[1] Federal Trade Commission, "National and State Trends in Fraud and Identity Theft," 22 January 2004.

[2] Fears, Darryl, "Southern U. Says Hundreds Altered Grades," *The Washington Post,* Washington, D.C., 2 April 2004, pg. A03.

[3] *Data Theft and Identity Protection*, 04 Nov. 2003, The University of Texas at Austin, 23 July 2004 <https://www.utexas.edu/datatheft/>

- In 2002, a student won a lawsuit he had filed against Gonzaga University in Spokane, Washington, for defamation based on that institution's release of confidential information.[4]

The University stores confidential data in various systems. Our audit focused on the protection of data in two of these systems: the Student Information Management System (SIMS) and the Financial Accounting Management Information System (FAMIS) (see text box). The University relies on controls at both the user level, such as passwords, and the enterprise level, such as firewalls, to protect these systems. Although the University has established generally adequate controls to protect confidential data and critical information systems from loss or unauthorized access and use, it does not consistently apply these controls, and other information system controls are not functioning as intended.

Student Information Management System

The University's Student Information Management System (SIMS) supports the administrative processing of student records for Texas A&M University and Texas A&M University at Galveston. The system processes admissions, registration, student financial aid, billing, grading, transcripts, degree audits, and student loan repayment.

Financial Accounting Management Information System

The Financial Accounting Management Information System (FAMIS) is a centralized accounting package maintained by the Texas A&M University System. FAMIS is used by 18 of the 21 Texas A&M University System component institutions, including Texas A&M University. FAMIS's functions include financial accounting, accounts receivable, accounts payable, fixed assets, annual financial reports, purchasing, sponsored research, and budgeting.

[4] Helm, Mark, "Supreme Court Hears Arguments in Gonzaga Privacy Case," *Seattle Post-Intelligencer*, 25 April 2002, Seattlepi.com, 23 July 2004 <http://seattlepi.nwsource.com/local/67884_gonzaga25.shtml>

Chapter 1

The University Should Address Weaknesses that Increase the Risk of Unauthorized Access

The University does not adequately review the user lists for its critical systems to ensure that all users are authorized and that their access is appropriate and necessary to perform their job duties. In addition, it does not consistently establish or enforce minimum requirements for the creation or maintenance of user passwords to reduce the risk of unauthorized access.

We also found that seven programmers for SIMS can make and approve changes to application code without an independent review. In addition, programming changes to FAMIS are documented manually for review purposes instead of tracked automatically. The monitoring of changes made to applications by programmers is critical because programmers have the ability to make changes that could affect all of the applications' data.

When SIMS is accessed remotely, user login IDs and passwords are not encrypted to prevent "eavesdroppers" from obtaining access to that information. In addition, the University does not consistently keep its servers properly configured or ensure that these servers have the most up-to-date security patches to prevent access by hackers.

Chapter 1-A

The University Does Not Always Ensure that Users' Access to Applications Is Necessary

We identified specific instances in which employees of the University and other individuals had unnecessary access to certain systems. To properly protect applications and related data, individuals should have access to critical University applications only to the extent necessary to perform their job duties.

The University does not always ensure that only current employees have access to applications.

We reviewed the current user lists for SIMS and FAMIS as of May 2004 and found that a number of employees still had access to these systems after they had left the University:

- Eighty-five of the more than 2,400 SIMS users still had access to SIMS after these users had left the University. Forty-six of these users had access from 1 to 12 months after they had left, while two more users had access for more than one year (one of these had access for more than two and a half years). Another 37 users had access after their departure, possibly for up to almost four years, but the University was not able to provide us with the mainframe access termination dates so we could be certain of how long these users had access after leaving the University.

Gaining Access to SIMS and FAMIS

To log in to SIMS or FAMIS, each user must have both an active mainframe access account and an active account for SIMS or FAMIS. If either of these accounts is not active, the user will not be able to log in to SIMS or FAMIS.

Of these 85 users, 12 accessed the system after their termination dates, but what they had accessed could not be determined. These 12 users had the ability to update students' course registrations; add or remove blocks to prevent students from receiving transcripts; and view information on grades, admission applications, biographic and demographic data, families, and financial assistance awards.

- Four of the more than 1,500 FAMIS users still had access to the University's financial accounts from four days to more than five months after leaving the University. None of these four users accessed FAMIS after their termination dates, although one of them had inquiry access to detailed payroll information.

The University uses an automated process periodically throughout the year to cancel mainframe accounts for employees not currently on the payroll and students not currently registered. Although this process does eventually cancel accounts that are no longer needed, accounts for users who leave the University between runs of this cancellation process may be active for several months afterward unless other action is taken.

The University does not always ensure that employees' access to applications is appropriate and necessary to perform their job duties.

In addition to ensuring that only current employees have access to critical applications, the University should ensure that all users of critical applications have only the access that they need. We found the following as of May 2004:

- Three SIMS users had unnecessary access to a key billing rate table, which they could have used to change tuition or fee rates for all students at the University. An erroneous decrease in these rates could have resulted in lost revenue, while an erroneous increase in these rates would have resulted in the University's inappropriately charging students too much. These users worked in the payroll department and had this access for 15 months after their job duties had changed.

- Two new mainframe user accounts with direct access to SIMS data were erroneously created with the ability to add unauthorized users with similar access. The University corrected this during our audit, and neither account had previously been used.

- One SIMS user (from a sample of 30 users tested) had a level of access to SIMS that exceeded his job duties for at least 21 months after his duties had changed. This user was a faculty member who served as chairman of his academic department until relinquishing those duties in August 2002. However, his access to SIMS was not adjusted when his duties changed.

Each year, University departments are provided a list of their users' access to SIMS (but no information on the type of access) and are asked to review the appropriateness of each user's access. The departments must indicate whether the employees listed on that report still work in the department or whether their access needs to be changed. However, the departments that are responsible for the SIMS data (Office of Admissions and Records, Office of the Registrar, Department of Student Financial Aid, and Student Financial Services) are not regularly required to review users' access to key data. Performing such a review might reduce the risk associated with unnecessary access as described above.

Our review of mainframe authentication found that access to inactive user accounts was not automatically revoked. Inactive user accounts indicate that the users do not use the access provided and may no longer need access to perform their job duties. Mainframe authentication is the first step in accessing FAMIS and SIMS, and inactive user accounts create the risk that an unauthorized individual could, without immediate detection, gain access through an authorized user's account.

We also found that 285 (18 percent) of the more than 1,500 current FAMIS users have either never used their accounts or have not used them in more than one year. FAMIS users are automatically prompted every 12 months to electronically acknowledge the FAMIS Statement of Responsibility in order to access FAMIS. These users are listed on a FAMIS report titled "FAMIS Users with Delinquent Statement of Responsibilities"; however, this list also may indicate that these users no longer need access to FAMIS.

Our network scans of selected domains (a group of network servers) also identified a large number of user accounts that the associated users had never used or had not used in more than 120 days. For two domains, up to 48 percent of the accounts had never been used or had not been used in more than 120 days. This may indicate that the users either never needed access or that they no longer need access.

Recommendations

The University should:

- Ensure that all users of critical applications are current employees whose job duties require access to those applications.

- Require departments responsible for SIMS data to identify key confidential data and regularly review users' access to this data.

- Change the mainframe authentication rule to revoke inactive user accounts after a specified period of inactivity.

- Review all applications and domains to identify user accounts that have never been used or that have not been used within a reasonable period of time (for example, within the past four months) and determine whether these accounts should remain active.

Management's Response

Management agrees that the current process of reviewing the continuing need for access can be improved. A committee will make recommendations to upper management on university rules and procedures for user access to critical applications. These procedures will include checks for changing job duties, terminations, and inactive accounts. The recommendations will be submitted to the university's upper management for approval by January 15, 2005.

Regarding access to SIMS data, the SIMS group is working with departments responsible for data elements (data owners) to enhance the account access report so it flags unusual access permissions such as having access to change tuition rate tables, etc. Both the data owners and the primary authorizing agents will review these reports each semester. The revised report will be implemented by January 15, 2005.

Chapter 1-B

Weaknesses in Password Policies and in the Enforcement of Password Policies Could Impair Data Security

A number of weaknesses in the University's password policies (see text box) and in the enforcement of those policies could impair the security of data. The proper protection and frequent changing of users' passwords are critical in protecting data. The establishment and enforcement of strong password policies also helps to protect data from unauthorized access.

What Is a Password Policy?

A password policy is the configuration of electronic settings defining how passwords are used on a given server. The password policy dictates how long and how difficult passwords should be, whether users have to change their passwords, the interval at which users should change passwords, whether passwords can be reused, and after how long an idle time users will be disconnected automatically.

Our scans of selected servers identified the following password weaknesses for user accounts:

- Password requirements for 26 (42 percent) of the 62 servers we scanned allowed passwords that were shorter than the recommended minimum length of six characters. Additionally, in our scans of specific domains (see below), three domains required password lengths ranging from zero to five characters. Passwords that are too short are more susceptible to compromise than longer passwords.

- Although we did not identify any accounts that lacked passwords, 27 (44 percent) of the 62 servers we scanned had accounts that did not require passwords. Two of those accounts were administrator accounts that could allow access to everything on the related servers. This weakness could allow future users to set up access to their accounts without passwords. Without a password, an unauthorized individual would need to know only an authorized user name to gain access to an account.

Our scans of specific domains and review of mainframe authentication rules identified the following password weaknesses for user accounts that could make it easier for unauthorized individuals to gain access to data:

- For three domains we scanned, the password policies for the maximum password age had been overridden; as a result, at least 90 percent of the passwords were set to never expire. However, for two of these domains this situation was temporary and was designed to reduce confusion because these domains were in the process of being combined into a single domain. If passwords are not set to expire, users are not prompted to change them regularly.

- The password requirements for three domains and for mainframe authentication were set to save only from zero to three passwords. If passwords are not saved in history, users could reuse the same ones repeatedly.

- For one domain, 10 accounts had passwords that were the same as the user names. In these cases, an unauthorized individual would need to know only an authorized user name to gain access to data.

- Complex passwords (using a combination of uppercase and lowercase letters, numbers, and special characters) were not required for mainframe authentication accounts. Simple passwords are more susceptible to compromise than complex passwords.

- Our scans of one domain used by the Department of Student Financial Aid identified no significant concerns related to user accounts.

Recommendations

The University should:

- Enforce all password policies and ensure that the policies require that:

  - All accounts on servers have passwords.

  - Passwords be at least six characters long.

  - To the extent possible, passwords include a combination of uppercase and lowercase letters, numbers, and special characters.

  - Passwords differ from the user names on the accounts.

  - Passwords expire after 90 days.

- Determine an acceptable period of time for passwords to be maintained in history to prevent their reuse, and include this requirement for all accounts.

Management's Response

Management agrees that strong passwords should be required on all systems. This requirement will be included in the development of the 22 TAC policies discussed in Chapter 2 of the audit report. The rules will be submitted for the university's approval process by January 15, 2005.

Chapter 1-C

The University Does Not Always Ensure that Changes to Applications Are Properly Authorized and Documented

Seven of the University's SIMS application programmers can both make and approve changes to the application's production libraries. Management was aware of the risk associated with this and determined that it was acceptable. In addition, the University uses software to track the changes that are made and identify the programmer who made the changes. However, if the logs from this software are not reviewed in a timely manner, unauthorized changes could exist for a long time before they would be detected and corrected. Segregation of duties among application programmers is critical to prevent unauthorized changes from being made to an application. Such changes, whether intentional or not, could cost the University revenue, damage its reputation, and increase the risk of fraud.

In addition, programming changes to FAMIS (which is maintained by the Texas A&M University System) are manually documented in the application code instead of automatically tracked in a separate system. Despite the requirement that all changes must be reviewed by at least one other person, it might be possible under current procedures for unauthorized changes to be implemented without those changes being manually documented. The Texas A&M University System plans to implement a new automated change-tracking software package by the end of February 2005. This will allow for improved tracking of code changes and different versions of the application.

Recommendations

The University should set up security in its change management software to require a second-level review of all SIMS code changes.

The Texas A&M University System should continue its plans to implement automated change-tracking software for FAMIS.

Management's Response

SIMS will modify the package approval rules for their change management software (Endevor & N2O) to require authorization by two SIMS team members (one being a senior staff member) before a package can be moved into production. This will be implemented by September 30, 2004.

The Texas A&M University System will continue its plans to implement automated change-tracking software for FAMIS by the end of February 2005.

Chapter 1-D

The University Does Not Always Ensure that Internal Access to Data Is Appropriately Secured

We identified instances in which the University did not properly protect data from unauthorized internal access. Unauthorized access to computer resources by external users is a widely publicized risk. However, the risk related to unauthorized access by internal users can greatly exceed that of access by external users because of internal users' familiarity with the operating environment and ability to access data without detection.

Specific access weaknesses for SIMS increase the risk of unauthorized access.

The University allows SIMS users to use Telnet (a protocol for accessing computers) and file transfer protocol (FTP, a standard file transfer protocol) to access SIMS and exchange data files. These methods communicate via plain text, which exposes the user's login ID and password to the risk of being captured by anyone "eavesdropping" on these network communications.

The University does not always keep servers updated with security patches or keep them properly configured.

Our technical scans identified critical vulnerabilities in network devices that can be addressed by installing the most current available security patches. Additional vulnerabilities could be eliminated if servers were properly configured and unnecessary services were turned off. During our audit, the University took the necessary actions to eliminate the critical vulnerabilities that we identified. Because some patches can cause problems with other University software, the University intentionally does not automatically apply all patches until after the patches have been tested.

Some of the vulnerabilities we identified increase the risk that an intruder could gain system-level privileges or the ability to access data, both of which could result in the unauthorized disclosure or destruction of confidential data. A compromised server could also serve as an intermediate point for launching additional attacks on the University’s main network.

In addition, we identified two domains for which the account lockout feature was not activated, potentially allowing a user to attempt to guess passwords for another user’s account for long periods of time without ever causing the account to deactivate. Although failed login attempts are captured in a log, someone would have to be actively monitoring the server to address an attempted intrusion. We also identified a third domain that was not logging security events such as failed logon attempts and, therefore, would not be able to detect attempts to hack into this domain’s servers.

Our scans of one domain used by the Department of Student Financial Aid identified no significant concerns related to patches and services.

Recommendations

The University should:

- Disable TelNet and FTP and implement a secure, encrypted method of access to SIMS.
- Review its server-patching process and determine what improvements can be made to keep systems patched.
- Verify that servers are configured correctly to eliminate unnecessary login accounts.
- Verify that services running on servers are necessary and either (1) patch and configure these services securely or (2) disable these services.
- Activate the account lockout feature on all servers and configure it to deactivate accounts after repeated unsuccessful login attempts.

Management's Response

A new telnet client has been acquired that implements encrypted access. It will be installed and deployed through the fall semester of 2004. Federal export restrictions disallow use of this client outside the United States, so an alternate approach will have to be found for Qatar. In any case, we will disable all unencrypted access by January 30, 2005.

Encrypted FTP is a feature of the most recent version of IBM's system. It will be installed by January 15, 2005. Note that the University currently encrypts some of the files that are transferred via FTP; those transfers are secure and will continue until/unless the recipients (e.g. financial institutions) change their encryption standards.

Management concurs with the remaining recommendations. The University will perform the recommended reviews and verifications, and the account lockout feature will be activated on confidential/critical information servers by December 15, 2004. Since the account lockout feature will leave some servers vulnerable to denial of service attacks from worms, we are developing an alternate strategy to handle such intrusion attempts. Thus the account lockout strategy may be replaced by a better way to mitigate this risk in the future.

Chapter 1-E

The University Does Not Always Ensure that External Access to Its Main Network and Data through Wireless Devices Is Appropriately Secured

The University has a generally strong wireless access program for its authorized wireless devices. It routes wireless network traffic to its own virtual local area network (VLAN), requires user authentication using a University ID, and encrypts all wireless traffic using a virtual private network (VPN).

However, 27 (42 percent) of the 64 wireless access points that we detected in selected University buildings on and off campus and at the Texas A&M University System Building were unauthorized. Because these access points were not authorized by the University, they may not be configured as securely as those installed by the University, which increases the risk that unauthorized users could gain access to the University's main network.

The University also has not activated the account lockout feature on its wireless authentication server. This could allow an intruder to attempt to guess passwords for an account for long periods of time without causing the account to deactivate. While failed login attempts are captured in a log, someone would have to be actively monitoring the server to detect and address an attempted intrusion.

Recommendations

The University should:

- Frequently scan to identify unauthorized wireless access points in University-occupied buildings (on and off campus) and take appropriate action to remove these access points or ensure that the security of these access points is adequate.

- Activate the account lockout feature on its wireless authentication server and configure it to deactivate accounts after repeated unsuccessful login attempts.

Management's Response

The University will add an additional network technician to the network troubleshooting team by December 15, 2004. The team will regularly scan and identify wireless access points and assure that they are authorized and secure.

The University will activate the account lockout feature on the wireless authentication server by September 30, 2004. Since this will leave the server vulnerable to denial of service attacks from worms, we are developing an alternate strategy to handle such intrusion attempts. Thus the account lockout strategy may be replaced by a better way to mitigate this risk in the future.

Chapter 1-F

External Scans of the University's Computer Network Identified No Vulnerabilities

Our external scans of the University's computer network did not identify any vulnerabilities. This is a result of the University's having a properly configured firewall/router in place that prevented us from accessing the servers we targeted.

Chapter 2

The University Should Ensure Compliance with Required Policies, Legal Requirements, and University Policies and Procedures

Compliance with applicable laws and regulations helps to ensure that data and computer resources are adequately protected. However, the University has not fully implemented on a University-wide basis most of the security policies required by the Texas Administrative Code (TAC). The University also does not monitor departments' progress to ensure that network users attend ongoing security awareness training as required by the TAC. However, the University has developed a good methodology for performing the risk assessment required by the TAC and the Safeguards Rule of the federal Gramm-Leach-Bliley Act of 1999 (GLB Act).

The University Lacks 16 of the 22 Information Security Policies Required by Texas Administrative Code, Title 1, Section 202.7(h)

The Texas Administrative Code requires that "each agency head or his/her designated representative and information security officer shall create, distribute, and implement information security policies. At a minimum, the … policies, will be developed and published based on the documented agency security risk management decisions and business function."

The University lacks required policies in the following areas:

- Account management
- Administrator/special access
- E-mail
- Incident management
- Internet/intranet use
- Intrusion detection
- Network access
- Network configuration
- Physical access
- Portable computing
- Security monitoring
- Security awareness and training
- Platform hardening
- Authorized software
- Vendor access
- Malicious code

The University has not implemented certain policies required by the Texas Administrative Code.

The University has not fully implemented on a University-wide basis 16 of the 22 information security policies that the TAC requires each agency or institution to create, distribute, and implement (see text box). Failure to comply with this requirement could expose the University's information resources to security weaknesses.

The University delegates responsibility for implementing these policies to the individual campus departments through a University rule. However, there is no overall monitoring in place to ensure that each department (and, therefore, the entire University) has the required policies in place. For example, the Department of Student Financial Aid, the Finance Division Computing Group, and the Office of Admissions and Records each adopted only a few of the required policies, and their selections of policies to adopt varied.

The University does not ensure that network users attend security awareness training.

The University does not have an ongoing security awareness education program for all users as required by the TAC, Title 1, Section 202.8(d). Although SIMS and FAMIS users receive security training when they initially obtain access to these systems, they do not receive any subsequent security awareness training. The University has delegated to departments the responsibility for determining what type of security awareness training will be administered, and it does not require the departments to use Web-based security awareness training that the University has developed. Departments are also responsible for tracking users' training to determine whether all users have received training; however, there is no overall monitoring of security awareness training at the University level.

The University has developed a good methodology for performing the risk assessment required by the TAC and the GLB Act.

The University requires each department to complete an annual risk assessment through its Information Security Awareness, Assessment, and Compliance (ISAAC) system, which addresses the risk assessment requirements of the GLB Act and TAC Section 202. The University's Computing and Information Services department reviews the departmental risk assessments along with institution-wide functions and forwards common or important issues to executive management for further action.

Recommendations

The University should:

- Fully implement all security policies required by the TAC on a University-wide basis. If responsibility for implementing these policies is left with the individual campus departments, the University should perform monitoring of the departments to ensure that the required policies have been implemented.

- Ensure that all network users attend security awareness training on an ongoing basis. This could be done by a mandate from executive management or by delegating this responsibility to the departments and regularly monitoring the departments' progress.

Management's Response

The university will create rules and standard administrative procedures applicable to all university departments, addressing all of the twenty-two areas listed in Texas Administrative Code 202 "Information Security Standards." These will be submitted for the university's approval process by December 15, 2004.

Training material for information security is being developed. A program to require ongoing training for all network users will be in place by January 15, 2005.

Chapter 3

The University Should Strengthen Disaster Recovery Plan Processes and Procedures for Critical Data and Applications

Improvements in the University's disaster recovery plan processes and procedures for critical data and applications would help to facilitate the recovery of the University's computer resources, including its confidential data, in the event of a disaster. Specifically, the University is not protecting its backup tapes of critical data from the risk of fire, although it has improved the location of its backup tapes. In addition, the University does not have written procedures for keeping its disaster recovery plan for critical data and applications current. It also does not adequately test this disaster recovery plan, nor does it have a formal plan for performing such tests.

The University does not adequately protect backup tapes of critical data from the risk of fire; however, it has improved its storage of backup tapes.

The University currently stores its backup tapes of critical data in a location that does not have a fire suppression system, and the tapes are not stored in a fireproof container. Therefore, these tapes could be destroyed if a fire were to occur, which could prevent the University from recovering data.

Creating backup tapes of critical data is an important step in any disaster recovery plan, but the protection of these tapes is just as important in ensuring that data will be accessible when it is needed. TAC, Title 1, Section 202.6(b) states that "Mission critical data shall be backed up … and stored off site in a secure, environmentally safe, locked facility."

The University recently moved the storage location for these backup tapes to the other side of campus, thus preventing a small disaster from damaging both the primary data center and the backup tapes. This resolves an issue that we noted in a prior report (see *A Financial Review of Prairie View A&M University,* SAO Report No. 04-009, November 2003).

The University has not developed procedures for testing and updating its disaster recovery plan for critical data and applications.

The University has not complied with requirements to annually test its disaster recovery plan for critical data and applications and does not have a formal plan to govern testing. Two planned tests of portions of the disaster recovery plan have been conducted since 1999 (both in 2000), and disaster recovery procedures have been implemented seven other times during the same time period in response to actual disaster incidents. The TAC, Title 1, Section 202.6(a)(5)(E), requires that the University test its disaster recovery plan annually. A test should be a planned exercise that is performed proactively to determine and correct potential weaknesses in the disaster recovery plan. This helps to ensure that all aspects of the plan are in place and that individuals know their duties when recovering from a disaster.

In addition, the University does not have a written policy or procedure for periodically reviewing and updating its disaster recovery plan for critical data and applications, although a designated Computing and Information Services administrator does review and revise the plan as needed. It is a good business practice to maintain written procedures for important operating functions to ensure efficiency and continuity of operation in the event of employee turnover. Keeping the disaster recovery plan current is critical to ensuring the prompt resumption of operations after a disaster.

Recommendations

The University should:

- Protect backup tapes of critical data from fire damage by storing them in a fireproof container or installing a fire suppression system in the storage room.
- Develop a plan for testing its disaster recovery plan for critical data and applications and test the plan at least annually, particularly for its most critical systems.
- Develop written procedures for reviewing and revising the disaster recovery plan for critical data and applications.

Management's Response

A fire suppression system will be installed in the storage room by December 15, 2004.

A regular procedure and schedule for testing disaster recovery plans will be developed by December 15, 2004.

Written procedures for reviewing and revising the disaster recovery plan will be completed by December 15, 2004.

Appendix

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether Texas A&M University (University) has adequate controls to protect confidential data and critical systems from loss or unauthorized access and use.

Scope

Our audit scope included general controls over all of the University's information systems and application controls for the University's Student Information Management System (SIMS) and its Financial Accounting Management Information System (FAMIS), as well as systems that share information with these two systems. Our scope covered controls in SIMS and FAMIS as of May 2004.

Methodology

Our methodology included interviewing staff, reviewing disaster recovery and information security plans and policies, inspecting major data centers, and conducting network and wireless scans to identify potential information systems vulnerabilities.

<u>Information collected</u> included the following:

- Policies and procedures applicable to user access, security, disaster recovery, and physical security
- Centrally managed information system network maps and diagrams

<u>Procedures and tests conducted</u> included the following:

- Interviews with key staff regarding user access, security, disaster recovery, and physical security
- On-site walk-throughs of areas that store major information system equipment
- Network scans using Internet Security Systems' (ISS) Internet Scanner and BindView's bv-Control for Windows and bv-Control for Netware scanning tools
- Limited wireless leakage tests using ISS Wireless Scanner, Airopeek Wireless Sniffer, Cirond Mobile AirPatrol, and Netstumbler
- Analysis of user access to FAMIS, SIMS, and the primary data center

<u>Information resources reviewed</u> included the following:

- Access and security controls for the centrally managed network, SIMS, and FAMIS

- Disaster recovery plans for the centrally managed network, SIMS, and FAMIS
- Physical security controls protecting the centrally managed network, SIMS, and FAMIS

Criteria used included the following:

- Texas Administrative Code, Title 1, Chapter 202 (Information Security Standards)
- The federal Family Education Rights and Privacy Act
- The federal Gramm-Leach-Bliley Act
- Texas Department of Information Resources guidelines

Other Information

We conducted fieldwork from March 2004 through June 2004. This audit was conducted in accordance with generally accepted government auditing standards. The following members of the State Auditor's staff performed this review:

- Paige Buechley, MBA, MPAff, CIA, CISA (Project Manager)
- Anthony W. Rose, MPA, CPA, CGFM (Assistant Project Manager)
- Michael Gieringer
- Lita Lacar, Ph.D.
- Jenay Oliphant
- Bill Wood, CPA, CISA
- Rodney Almaraz, MBA, CPA, CISA (Information Systems Audit Team)
- Gary Leach, MBA, CQA (Information Systems Audit Team)
- Michael Yokie, CISA (Information Systems Audit Team)
- Leslie Ashton, CPA (Quality Control Reviewer)
- Ron Franke, MBA, CISA (Audit Manager)
- Frank Vito, CPA (Audit Director)

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable David Dewhurst, Lieutenant Governor, Joint Chair
The Honorable Tom Craddick, Speaker of the House, Joint Chair
The Honorable Steve Ogden, Senate Finance Committee
The Honorable Thomas "Tommy" Williams, Member, Texas Senate
The Honorable Talmadge Heflin, House Appropriations Committee
The Honorable Brian McCall, House Ways and Means Committee

Office of the Governor

The Honorable Rick Perry, Governor

Board of Regents of the Texas A&M University System

Mr. Lowry Mays, Chairman
Mr. Erle Nye, Vice Chairman
Mr. Phil Adams
Dr. Susan Rudd Bailey
Dr. Wendy Gramm
Mr. Bill Jones
Mr. Lionel Sosa
Mr. R.H. (Steve) Stevens, Jr.
Mr. John D. White

Texas A&M University System

Mr. A. Benton Cocanougher, Interim Chancellor

Texas A&M University

Dr. Robert M. Gates, President

In compliance with the Americans with Disabilities Act, this document may also be requested in alternative formats. To do so, contact our report request line at (512) 936-9880 (Voice), (512) 936-9400 (FAX), 1-800-RELAY-TX (TDD), or visit the Robert E. Johnson Building, 1501 North Congress Avenue, Suite 4.224, Austin, Texas 78701.