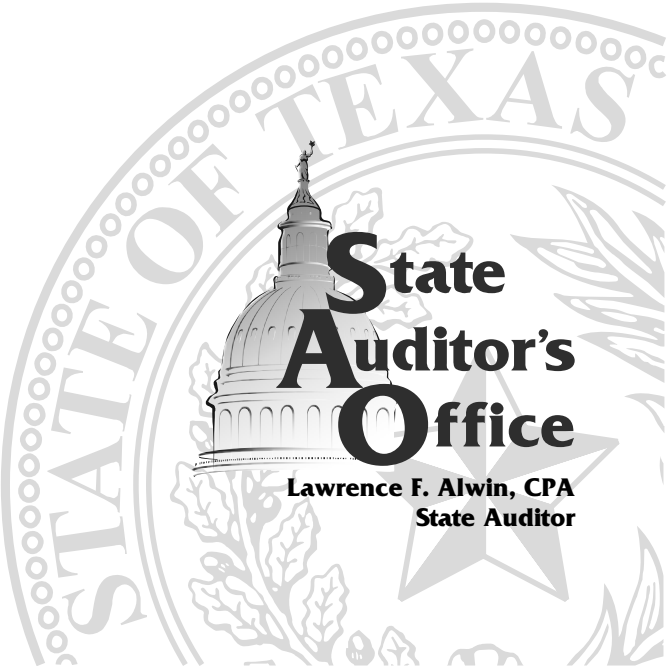
An Audit Report on

The Protection of Confidential Information and Critical Systems at the University of Houston

November 2004

Report No. 05-010



State Auditor's Office

Lawrence F. Alwin, CPA
State Auditor

An Audit Report on

The Protection of Confidential Information and Critical Systems at the University of Houston

SAO Report No. 05-010
November 2004

Overall Conclusion

Although the University of Houston (University) has implemented certain controls, it needs to implement additional controls to ensure that it adequately protects confidential information and critical systems. The University collects and stores a significant amount of confidential information in automated systems. We did not identify any breaches of security or disclosure of confidential electronic data, but we did identify weaknesses that the University needs to address to ensure that its information and systems are adequately protected. Specifically:

Systems Audited

Student System: This system is an integrated, multi-campus enrollment management system that comprises recruiting, admissions, records and registration, advising, student financials, and data extraction applications.

PeopleSoft Public Sector Human Resources System (HR/Payroll System): This system collects and stores employee information such as Social Security numbers, salary information, and other personal information.

Cougar1 Card System: This system is the campus picture ID/library/debit card system.

- The University does not always ensure that high-level user accounts, which allow access to and control of a broad range of systems and information, are used appropriately. It also does not always monitor activity conducted through these high-level user accounts.
- The University exchanges information through methods that are not secure, and weaknesses in wireless access increase the risk of unauthorized access. Although the security of the University systems we audited is generally adequate, network monitoring could be enhanced.
- The University does not always remove or change user access as needed, which increases the risk of unauthorized access. Weaknesses in passwords also increase this risk.
- Weaknesses in disaster recovery and business continuity planning increase the risk that the University would be unable to promptly and fully recover from a disaster. In addition, specific weaknesses in physical security increase the risk that network equipment is not adequately protected. Also, the University's information security program does not meet certain requirements of the Texas Administrative Code.

Summary of Management's Response

The University generally agrees with our recommendations.

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 Carol Smith, Audit Manager, at (512) 936-9500.

Summary of Information Technology Review

We focused on the security of confidential data in the University's Student System, PeopleSoft Public Sector Human Resources System (HR/Payroll System), and Cougar1 Card System, as well as on the University's management of central information resources. We conducted network 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 University's financial system because the University was in the process of upgrading that system's software; however, we did review the process the University used to upgrade and test the new version of that software.

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.

The scope of our audit was limited to the Student System, the HR/Payroll System, and the Cougar1 Card System.

Our methodology consisted of reviewing University system and main campus policies and procedures and the disaster recovery plan, conducting interviews with staff, inspecting locations at which computing equipment is stored, and reviewing system settings and accounts. We also performed limited network vulnerability scans and searched for unauthorized wireless access points on campus.

Contents

Detailed Results

Appendix

Detailed Results

Introduction

The University of Houston (University) collects and stores a significant amount of confidential information in automated systems. For example, the University collects personal information for its more than 35,500 students such as Social Security numbers, grades, medical information, financial information, and information about students' parents. It also collects personal information for its more than 8,300 full- and part-time employees. Although the University has implemented certain controls, it needs to implement additional controls to ensure that it adequately protects its confidential information and critical systems. We did not identify any breaches of security or disclosure of confidential electronic data, but we did identify weaknesses that the University needs to address to ensure that its information and systems are adequately protected.

It is critical that the University protect this information for several reasons. Federal laws such as the Family Educational Rights and Privacy Act (FERPA) and the Gramm-Leach-Bliley Act (GLBA) require the University to safeguard certain data (see text box). Although FERPA and GLBA impose no monetary fines for disclosure of confidential information, universities are required to notify individuals when their confidential information may have been disclosed; therefore, universities can still incur costs to make this notification. For example, hackers were able to compromise computers containing Social Security and driver's license numbers at the University of California – San Diego. This university subsequently notified 380,000 students, alumni, applicants, staff, and faculty about this incident.[1]

Federal Laws Requiring Protection of Information

The **Family Educational Rights and Privacy Act** (FERPA) is a federal law that protects the privacy of student education records. Universities must have written permission to release any information from a student's education record except for certain "directory" information.

The **Gramm-Leach-Bliley Act** (GLBA) establishes standards to ensure the security and confidentiality of student financial records and information.

In addition, the unauthorized disclosure of confidential data could lead to civil lawsuits from individuals who suffer damages. For example, 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.[2]

The University's reputation could also be harmed as a result of the unauthorized disclosure of or failure to limit access to confidential or critical 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.[3]

---

[1] Yang, Eleanor, "UCSD says computer server hit by hackers," *San Diego Union*, 7 May 2004, SignOnSanDiego.com, <http://www.signonsandiego.com/uniontrib/20040507/news_7m7breach.html>

[2] 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>

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

Hackers are attracted to universities because of their large computing resources and relatively open environments. In addition, storing student and employee records electronically makes it easier for hackers to access an extensive number of records at one time.

Systems Audited

Student System: This system is an integrated, multi-campus enrollment management system that comprises recruiting, admissions, records and registration, advising, student financials, and data extraction applications.

PeopleSoft Public Sector Human Resources System (HR/Payroll System): This system collects and stores employee information such as Social Security numbers, salary information, and other personal information.

Cougar1 Card System: This system is the campus picture ID/library/debit card system.

The increase in cases of identify theft also 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.[4]

Our audit focused on confidential information that the University stores in its Student System, its PeopleSoft Public Sector Human Resources System (HR/Payroll System), and its Cougar1 Card System (see text box).

During our audit, the University upgraded its financial system to PeopleSoft Version 8. We reviewed the process the University used to upgrade and test the new version. We also reviewed access controls on the HR/Payroll System and the Student System. In addition, we reviewed how the University uses perimeter controls to prevent unauthorized access from outside the institution.

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

We identified weaknesses associated with the use and management of user accounts with a high level of access that increase the risk of fraud and unauthorized access to the Student System and HR/Payroll System. In addition, the University does not monitor access logs for these accounts or review changes to critical data to ensure that these accounts are used appropriately and have not been compromised.

Chapter 1-A

The University Does Not Always Ensure that High-Level User Accounts Are Used Appropriately

Specific weaknesses in the use and management of high-level user accounts increase the risk of fraud and unauthorized access to the Student System and HR/Payroll System. High-level accounts generally provide users with widespread capabilities to extensively modify data and applications. We identified the following weaknesses:

- **Staff working as database administrators also have access to system security functions.** This is a violation of University policy and increases the risk that unauthorized access to confidential information and critical systems could go undetected. A database administrator for the HR/Payroll System also has access rights to set up user accounts in that system. In addition, database administrators for the Student System have access to this system's security function, which is a violation of separation-of-duties principles. This could allow a database administrator to both create and use a high-level user account through the application and directly modify data in order to process inappropriate or fraudulent transactions. To ensure that changes are adequately tracked and that users are held accountable for those changes, the same individual should not be allowed to both make changes directly to the database and make changes through the application.

Examples of High-Level User Accounts

Security administrators have a wide range of authority within the application to set up user accounts and grant users access.

Database administrators manage the structure and integrity of databases as a whole through a database management program and not through the application.

- **Accounts with high-level access are not removed in a timely manner.** We identified three users who had high-level access to the Student System up to three years after they no longer needed this access. It is critical that the University remove such accounts promptly because these accounts can be used to make extremely significant and widespread changes to systems and data. For example, these accounts could be used to expand a user's access to the Student System.

- **Users do not always file proper authorization documentation.** Seven (33 percent) of 21 high-level users of the HR/Payroll System that we tested did not have proper documentation on file authorizing them to have high-level access, as required by University policy. These users have extensive access to applications and processes that allow them to make corrections and updates to all records.

- **Users share high-level user IDs and passwords.** The database administrators for the HR/Payroll System share the same user ID and password to make administrator-level changes. In addition, one of the users with a high-level access account for

the Student System is deceased, but staff continue to use this individual's user ID and password to run certain batch processes. Because users share this account, the University would not be able to hold a specific individual accountable for making inappropriate changes to databases and applications because it would not be able to identify which user used the account when a particular change was made. University policy requires that all actions, either online or batch, should be "fully auditable to an individual."

Recommendations

The University should:

- Ensure that database administrators do not have access to security functions and other applications. If implementing separation of duties is not practical, the University should implement regular supervisory reviews of security logs and changes to applications and databases made by database administrators.
- Periodically review high-level user accounts to ensure that those accounts are still necessary.
- Ensure that users have proper authorization documentation and approval to obtain high-level access.
- Ensure that each user has his or her own unique user ID and password and that users do not share these IDs and passwords.

Management's Response

We will review the separation of database administrator (DBA) duties and implement changes to ensure that DBAs do not have access to security functions and other applications by January 31, 2005. Where separation of duties is not practical, appropriate supervisory reviews will be implemented at the same time.

Annual reviews of high-level user accounts will be performed commencing January 31, 2005.

To ensure that high-level users always have proper authorization documentation, internal procedures shall be reviewed and corrected by January 31, 2005.

We will assess our situation regarding high level user IDs and passwords and develop an action plan for providing a fully auditable environment by individual by March 31, 2005. This action plan should be completed by August 31, 2005.

Chapter 1-B

The University Does Not Always Monitor Activity Conducted through High-Level User Accounts

Application owners for the Student System and the HR/Payroll System do not review access logs to identify failed access attempts or other security events to ensure that high-level accounts have not been compromised. This is particularly important for

the HR/Payroll System because the version of the software (PeopleSoft 7) underlying that system does not have an account-lockout feature. The absence of a lockout feature could allow a hacker to continually try to guess a password without being locked out of the account. Anyone who successfully guessed a password would have high-level access that could allow him or her to change or delete HR/Payroll System data, such as salaries.

The HR/Payroll System also does not require users to change their passwords or use passwords that are of an appropriate length and complexity. While there are logs of activity conducted in the HR/Payroll System, when the University cleans a log file, it eliminates log data prior to a certain date to free up space to hold more recent log data. Because log data is eliminated, there is a risk that unauthorized access and changes would not be reflected in the logs. The operating system log for the Student System does not capture user ID or Internet protocol address information that would help identify the user.

University departments also do not review changes to critical information to ensure that high-level accounts are used appropriately. Specifically, University departments do not review significant changes that users make to information such as grades or degree status in the Student System. The Registrar's Office can create a report of all changes made, but that report does not show how the information appeared before and after the changes were made. Reviewing this information is important because of the number of users who have the ability to change critical information. For example, 16 users can access and change student grades.

Recommendations

The University should:

- Monitor the access logs for high-level user accounts for specific security events (such as account lockouts or repeated unsuccessful logins) to ensure that these accounts have not been compromised.

- Review changes to critical data to ensure that these changes are appropriate.

Management's Response

Information Security personnel will begin a monthly review of the access logs for high level accounts to insure account integrity. This process will be in place by February 1, 2005.

We will identify critical data in the HR/Payroll and Student systems and establish additional procedures, as necessary, to review changes made to this data by March 31, 2005.

Chapter 2

The University Should Ensure that Information Is Exchanged through Secure Methods

The University exchanges certain information through methods that are not secure and is working to address this issue by upgrading its software. Weaknesses in wireless access also increase the risk of unauthorized access. Although the security of the University systems we audited is generally adequate, network monitoring could be enhanced.

Chapter 2-A

The University Exchanges Certain Information through Methods that Are Not Secure

The University shares files using file transfer protocol (FTP). This process does not encrypt the files, which increases the risk of unauthorized access to this data. When individuals use FTP, the data is exchanged in clear text (actual text of letters, numbers, and characters), which (1) exposes the data to the risk of being captured by anyone "eavesdropping" on the communication and (2) allows the data to be easily viewed. Encrypted file-sharing is possible with FTP, but only if the other party to the transmission supports that function.

The Student System exchanges unencrypted information with other University systems or external parties using FTP. The information exchanged through these processes includes student financial aid and income tax data. We identified 25 exchanges of information. Sixteen of the 25 exchanges were with other University systems and, therefore, were exposed to the risk of unauthorized internal access. The remaining nine exchanges were with external parties and were transmitted via the Internet; therefore, these exchanges were exposed to the risk of unauthorized internal and external access.

Users of the Student System access this system through Telnet, which transmits user IDs and passwords in clear text. Because user IDs and passwords are not encrypted, the risk that unauthorized individuals could intercept a user ID and password and access the Student System is increased. The University is in the process of reducing this risk by installing software that would encrypt this information.

Recommendations

The University should:

- Work with external parties to ensure that information is exchanged securely.
- Disable FTP and Telnet and implement a more secure or encrypted method of file transfer and system access.
- Continue implementing software to encrypt Student System user IDs and passwords.

Management's Response

We are working with the external parties to help ensure that information is exchanged securely. This process will be completed by June 30, 2005.

We are initiating a process to provide a transition in the Student System from FTP and Telnet to a secured environment. This process may include upgrades to software and hardware, including desktops, and it will have to be communicated to users and they will have to be trained. Non-secure FTP and Telnet will be disabled by December 31, 2005 with the most sensitive transfers being completed first.

Implementation of software to encrypt Student System user IDs and passwords will be completed by December 31, 2005.

Chapter 2-B

Weaknesses in Wireless Access Increase the Risk of Unauthorized Access

The University does not require users who access its wireless network to log in through a user account with a user ID and password. When users connect to the University's wireless network, they are not allowed to access the Internet, but they can still access devices and computers inside the University's network. This means that unauthorized individuals can pick up a wireless signal from the University's campus to access or potentially scan network resources without logging in. We verified this by using wireless devices to connect to devices on the University's network while we were in a campus parking lot.

The University also does not always encrypt data that users transmit through wireless devices. After an individual connects to the University's wireless network, the data that is transmitted is not encrypted unless the individual is using an application that provides for encryption. This increases the risk that unauthorized individuals could capture and view data by monitoring network traffic. Although the University provides a virtual private network (VPN) that protects the broadcasts of a wireless device from "eavesdropping" through other wireless devices in the same area, users must use the VPN only if they wish to access the Internet.

We also identified several unauthorized wireless access points that expose the University's network to the risk of intrusion. Thirty-three (23 percent) of the 145 wireless access points we identified were unauthorized or were not configured according to the authorized specifications and, therefore, were assumed to be unauthorized.

Furthermore, all of the University's authorized wireless access points use the same service set identifier (SSID), which was the vendor's default SSID. This makes it difficult to distinguish between authorized and unauthorized wireless access points.

Recommendations

The University should:

- Require all users of the wireless network to authenticate their identities using a user ID and password. This could be accomplished by redirecting all wireless access to an authentication page that requires the users to log in prior to allowing any access to the Internet or University network resources.

- Require users to connect to the wireless network using the VPN or other applications that provide for encryption of data.

- Rename all of its authorized wireless access points from the default SSID to a unique name.

Management's Response

The University will require all faculty, staff and student users of the authorized wireless network to authenticate their identities using a user ID and password by August 31, 2005. Campus Guests (art galleries, meeting visitors, athletic spectators, visiting lecturers, etc.) will be provided restricted access to public resources by completing a registration process.

The University will ensure that all critical systems identified in the scope of this audit will only accept a campus LAN (hardwired) or other connections (wireless or off-campus) utilizing the VPN (authenticated and encrypted) service by August 31, 2005.

As part of the University's wireless upgrade project, the University will also rename all of its authorized wireless access points from the default SSID to a unique name. This will be completed by August 31, 2005.

Chapter 2-C

Although the Security of the University Systems We Audited Is Generally Adequate, Network Monitoring Could Be Enhanced

Overall, our network scan results showed that the University is generally installing necessary security updates and patches to correct problems in and protect the HR/Payroll System, the Student System, and the Cougar1 Card System. However, we did identify some information resources with high vulnerabilities that could affect these three systems' availability. We shared the detailed results of our scans with the University, and it reports that it is addressing the vulnerabilities that the scans identified. Although the University has the same scanning tools that we used, it does not use these tools regularly.

In addition, our scans showed that the University is limiting external access to critical resources and is limiting these resources' exposure to outside attacks. Some of the resources we scanned were not accessible from the Internet; others were protected because they were behind the University's newly implemented firewall.

However, the University could do more to monitor network traffic. The University has an intrusion-detection system at its perimeter to monitor network traffic, but it has only one device that is monitoring traffic. Given the size and complexity of the University's network, having additional devices to monitor traffic could improve network management. In addition, the University does not monitor internal network traffic using its intrusion detection system. Monitoring traffic, particularly internal traffic, helps to detect and prevent attacks from spreading through the network.

Recommendations

The University should:

- Continue to install patches as needed.
- Use its scanning tools on a regular basis.
- Consider improving its monitoring of network traffic through the installation of additional intrusion-detection devices and increased monitoring of internal traffic.

Management's Response

The University will continue installing patches as needed.

The Information Security department will establish a schedule to regularly scan the University network for vulnerabilities. This schedule will be established by February 1, 2005, and will include the frequency with which we will scan the network or specific sections of the network.

The Information Security department will review the viability and resources required to expand internal network monitoring utilizing IDS tools and create an action plan by June 30, 2005.

The University does not always remove or change user access as needed, which increases the risk of unauthorized access. Weaknesses in passwords also increase the risk of unauthorized access. Having strong user access and password controls helps to reduce the risk that user accounts could be compromised.

Chapter 3-A

The University Does Not Always Remove or Change User Access as Needed, which Increases the Risk of Unauthorized Access

Because the University does not always remove or change system user access as needed, the risk of unauthorized access to its HR/Payroll System, the Student System, and CougarNet—the University's primary domain—is increased. After we informed the University about user accounts that we had identified as being associated with users who no longer needed access, the University reported that it had disabled these accounts.

What Is CougarNet?

CougarNet is the University's primary domain that gives users access to e-mail and many other resources on the network. It does not provide direct access to the Student System or HR/Payroll System.

Specifically, we found that:

- A total of 111 (15 percent) of the 727 HR/Payroll System users no longer needed access to that system. Of these users, 105 had been terminated, and the University could not find any information for the other 6 users in its human resource system. Seven of the 105 accounts associated with terminated users had been used to access the system after the associated users' termination dates. One of these accounts had been used to access the HR/Payroll System more than a year and a half after the associated user had been terminated from the University. The University reported that it had disabled these 111 accounts.

- Twenty-four (2.2 percent) of the 1,087 users of the Student System no longer needed access to that system. Sixteen of these users had been terminated. Other staff members were still using 1 of those 24 accounts to perform batch processes. In addition, 6 of these 24 accounts were for individuals who were never University employees, and the security administrator was not notified by the individuals' sponsoring departments that these accounts needed to be disabled.

- We found that, of the 39,720 CougarNet user accounts:

  - 19,559 (49 percent) had never been used. This is a significant risk because the user IDs and passwords for these accounts are initially in a standard format. The existence of accounts that have never been used and still have passwords in the standard format makes it easier for an unauthorized individual to guess the password and use one of these accounts to access information and systems without detection. One of these accounts had system-administrator–level access.

  - 4,053 (10 percent) had a last log-in date that was as least 120 days in the past. The oldest last log-in date was in June 2003. One of these accounts had system-administrator–level access and had not been used since December

2003. If the University does not identify and remove "stale" accounts such as these, the risk that an unauthorized individual could use one of these accounts to access information and systems without detection is increased. If an intruder used one of these accounts, it would be difficult for the University to detect this type of unauthorized access.

The University's policies require departments to annually review their employees' access to University information systems and applications, verify that each employee has the appropriate level of access, and report this information to the University's information security officer. However, this does not occur. The HR/Payroll System does not have an automated process to remove users' access to this system based on their employment status. Although the University has a process to automatically remove users' accounts from the Student System when users are no longer current employees, this process does not always work properly. This process also does not capture information on employees who change positions within the University. University departments are responsible for notifying application owners or administrators about employee terminations or job changes. However, departments do not always review user access periodically to determine whether the level of access users have is still appropriate.

Further, when employees leave the University, their departments are required to submit a Termination Check List to the Human Resources department that documents the request to disable the employees' access to systems. However, we reviewed Human Resources' files for 28 terminated users and found that only 10 of these files contained these checklists. Of these 10 checklists, 2 did not have the required signature authorizing the request to disable the user's access.

Recommendations

The University should:

- Develop, implement, and enforce procedures for disabling accounts for all systems when users no longer need access. This process should cover users who leave the University or change jobs within the University.

- Review the list of stale user accounts and disable or remove all accounts for employees, students, and other users who do not use their accounts or who are no longer associated with the University.

Management's Response

New procedures for disabling and removing accounts will be developed, implemented, and enforced by July, 2005. These procedures will cover users who leave the University or change jobs within the University.

A review of all stale accounts will be conducted and accounts will be disabled and removed by December 17, 2004.

Chapter 3-B

Weaknesses in Passwords Increase the Risk of Unauthorized Access

The University's information security policies allow passwords for automated systems to be only five characters in length, which is too short to allow for adequate protection from unauthorized access. In addition, under the University's current version of PeopleSoft, the HR/Payroll System does not have password controls such as minimum password length and complexity, required password changes, or an account lockout feature. Some of these weaknesses can be addressed when the University upgrades to a new version of PeopleSoft.

While the password controls in the Student System were generally strong, we identified password weaknesses in other systems that increase the risk of unauthorized access.

- **Inadequate password length.** Passwords for the CougarNet and the VPN are required to be a minimum of only five characters. In contrast, the Student System requires users to have passwords that are between 10 and 32 characters.

- **Lack of password complexity.** The passwords for CougarNet and the VPN do not have to be complex passwords that include letters, numbers, and special characters. The Student System allows passwords to include numbers, but it does not require users to create complex passwords.

- **Failure to maintain password history.** Users are required to change their CougarNet passwords every 60 days. However, because CougarNet does not maintain password history, users can reuse the same password. In contrast, the Student System requires users to change their passwords every 60 days, and it maintains password history and prevents their reuse for one year.

Recommendations

The University should:

- Revise its information security policies to require that, where possible, passwords be at least eight characters in length.

- Until the HR/Payroll System is upgraded, consider using a third-party product that would enforce stronger password controls and require users to change their passwords.

- Ensure that, when possible, systems require the use of passwords that are at least eight characters in length and that are composed of letters, numbers, and special characters.

- Ensure that CougarNet maintains password history to prevent users from reusing the same password.

Management's Response

The Information Security Manual has been revised to require eight character passwords and to include the use of letters (upper and lower case), numbers and special characters when possible.

The upgrade of the HR/Payroll system to Version 8 is complete.

Implementation of passwords that are at least eight characters in length and that are composed of letters, numbers, and special characters will be completed by December 31, 2005.

Processes which preclude maintaining password history will be modified and CougarNet password history will be implemented by August 31, 2005.

Weaknesses in disaster recovery and business continuity planning increase the risk that the University would be unable to promptly and fully recover from a disaster. Specific weaknesses in physical security also increase the risk that network equipment is not adequately protected. In addition, the University's information security program does not meet certain requirements of the Texas Administrative Code.

Chapter 4-A

Weaknesses in Disaster Recovery and Business Continuity Planning Increase the Risk that the University Would Be Unable to Promptly and Fully Recover from a Disaster

The University has developed a written disaster recovery plan for information resources. It also stores backup media containing critical data (including data from the HR/Payroll System and Student System) off-site in a secure, environmentally safe, locked facility. However, the University has not fully tested its disaster recovery plan to ensure that it would be able to maintain or quickly resume mission-critical functions. The Texas Administrative Code requires that disaster recovery plans be tested annually.

Texas Administrative Code, Section 202.6, Business Continuity Plan Elements

- **Business impact analysis** to systematically assess the potential impacts of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from various events or incidents.
- **Security risk assessment** to weigh the cost of implementing preventative measures against the risk of loss from not taking action.
- **Recovery strategy** to appraise recovery alternatives and alternative cost estimates.
- **Implementation, testing, and maintenance management program** addressing the initial and ongoing testing and maintenance activities of the business continuity plan.
- **Disaster recovery plan** for information resources.

During our audit, the University conducted a walk-through of its disaster recovery plan. While this exercise was useful because staff identified areas for improvement, it did not test some critical elements of the plan such as whether the University's current "cold sites" have the capacity to operate adequately.

In addition, the University has not developed a written business continuity plan that covers all of its business functions (see text box for the requirements for this plan). Although the University has an emergency management plan, that plan does not directly address information resources. The University also has not conducted a business impact analysis to assess the potential effects of a loss of business functionality due to an interruption of computing and/or infrastructure support.

Recommendations

The University should:

- Test its disaster recovery plan on an annual basis to ensure that the plan is adequate.

- Develop a comprehensive business continuity plan that covers all business functions and incorporates all requirements of the Texas Administrative Code, including a business impact analysis.

Management's Response

By August 31, 2005 we will modify our procedures to require a systematic test of the disaster recovery plan annually.

In the Summer of 2001 we successfully recovered from Tropical Storm Allison and were able to get all critical services running within 7 days. After this disaster we realized that our previous plan was not adequate and we decided to continuously review and modify the plan. The University will review and modify, as necessary, the existing business continuity plan to ensure that it adequately addresses the requirements in Texas Administrative Code, Section 202, Business Continuity Plan Elements by August 31, 2005.

Chapter 4-B

Specific Weaknesses in Physical Security Increase the Risk that Network Equipment Is Not Adequately Protected

Although the University has adequate physical security for critical information systems (including the HR/Payroll System and Student System) in its Computing Center, it should ensure that other facilities that house or will house critical network equipment are safe from environmental hazards.

For example, during our audit, the University was in the process of moving some network equipment from a room that experienced severe flooding during Tropical Storm Allison to another room. However, the room to which the University was moving this equipment lacked an alarm system, had a door that led to a classroom, and had an inadequate door lock.

Recommendation

The University should ensure that all areas in which information resources are stored are adequately protected from environmental hazards and theft.

Management's Response

The University has processes in place to ensure all of its central areas in which information resources are stored are adequately protected from environmental hazards and theft. As vulnerabilities are identified they are prioritized and addressed. The items cited by the SAO as examples have been resolved.

Chapter 4-C

The University's Information Security Program Does Not Meet Certain Requirements of the Texas Administrative Code

The University's information security program is not in compliance with certain information security standards required by Chapter 202 of the Texas Administrative Code.

The University has not updated its security program.

The University lacks an up-to-date security program as required by Texas Administrative Code, Section 202.2(2), and the federal Gramm-Leach-Bliley Act (GLBA). Although the University previously addressed the elements of a security program within its security manual, it has not updated this manual in several years. The University has completed a risk assessment to determine compliance with GLBA and has identified actions it needs to take to improve its security program.

The University lacks an ongoing security awareness training program for all users.

The University does not have a formal security awareness training program for all users as required by Texas Administrative Code, Section 202.8(d). Although users with access to the HR/Payroll System and Student System complete training that includes limited security information when they initially receive access to these systems, the University does not formally provide this training on an ongoing basis.

Although the University does not have a formal security awareness training program, it does provide security awareness information. For example, the University provides security information for users on its Web site and publishes articles in the campus newspaper. In addition, users of the Student System see a statement when they log on to this system that notifies them that unauthorized access is prohibited and directs them to the information security policies.

The University does not require all users to acknowledge their responsibility to comply with security requirements.

Although the users of the Student System, the HR/Payroll System, and CougarNet sign acknowledgements when they first receive access, the University does not require users of its other information resources to formally acknowledge that they will comply with the University's security policies and procedures as required by Texas Administrative Code, Section 202.8(a). When users request access to the Student System, the HR/Payroll System, or CougarNet, they sign agreements acknowledging that they will abide by University security policies.

The University's information security officer does not report to executive management.

The University's information security officer does not report to executive level management as required by the Texas Administrative Code, Section 202.3(d). This rule also requires the information security officer to report (at least annually) to the University's president on the status and effectiveness of information resources security controls. However, the University's information security officer does not currently provide this information to the president. Complying with these

requirements is important in ensuring that executive management has an awareness of (1) security risks facing the University and (2) how the University is responding to those risks. It also helps to ensure that executive management makes informed decisions about information security risks.

Recommendations

The University should:

- Update its security program.
- Develop and implement an ongoing security awareness training program for all users. This program could be modeled after other programs in use at other institutions or programs developed by higher education information technology associations.
- Require all users to acknowledge their responsibility to comply with security requirements. It should also determine the method of acknowledgement and determine how often users must re-execute this acknowledgement.
- Require its information security officer to report to the appropriate level of management. At least annually, the information security officer also should report to the University's president on the status and effectiveness of information resources security controls.

Management's Response

The Information Security department is in the process of updating the security program in order to incorporate the requirements of GLB, TAC202 and other regulations. In addition, IT is nearing the final stages of developing new policies and procedures for the University in regards to information security. This process should be completed by August 31, 2005.

Information Security has begun working with IT Support Services in order to develop an information security awareness training program. We anticipate the program will be available for use by August 31, 2005.

The Information Security department will establish a mechanism to ensure users' acknowledgment of responsibilities, and to determine how often this acknowledgment will be required to be renewed. This acknowledgment will be in the form of a Notification or Certificate of Completion of the previously mentioned awareness training program. This should be in place by August 31, 2005.

The information security officer will report to the appropriate level of management by December 31, 2005. Also, by June 30, 2005 the information security officer will report to the UH president on the status and effectiveness of the information resources security controls on an annual basis thereafter.

Appendix

Objective, Scope, and Methodology

Objective

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

Scope

The scope of our audit was limited to the Student System, the PeopleSoft Public Sector Human Resources System (HR/Payroll System), and the Cougar1 Card System.

Methodology

Our methodology consisted of reviewing University system and main campus policies and procedures and the disaster recovery plan, conducting interviews with staff, and reviewing system settings and accounts. We also performed limited network vulnerability scans and searched for unauthorized wireless access points on campus.

Information collected included the following:

- Policies and procedures applicable to user access, security, disaster recovery, and physical security
- Centrally managed information system network maps and diagrams
- User and employee lists
- Information on system upgrade processes

Procedures and tests conducted 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

Information resources reviewed included the following:

- Access and security controls for the centrally managed network, the Student System, the HR/Payroll System, and the Cougar1 Card System
- Disaster recovery plans for the centrally managed network, the Student System, the HR/Payroll System, and the Cougar1 Card System
- Physical security controls protecting the centrally managed network, the Student System, the HR/Payroll System, and the Cougar1 Card System

Criteria used included the following:

- University policies and procedures
- 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

Project Information

Our fieldwork was conducted from June 2004 to September 2004. We conducted this audit in accordance with generally accepted government auditing standards. The following members of the State Auditor's staff conducted this audit:

- Paige Buechley, MBA, MPubAff, CIA, CISA, Project Manager
- Anthony Rose, MPA, CPA, CGFM, Assistant Project Manager
- Vicki Durham
- Michael Gieringer
- Gary Leach, MBA, CQA, Information Systems Audit Team
- Jenay Oliphant
- Michael Yokie, CISA, Information Systems Audit Team
- Rodney Almaraz, MBA, CPA, CISA, Information Systems Audit Team
- Leslie Ashton, CPA, Quality Control Reviewer
- Ron Franke, MBA, CISA, Audit Manager

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 University of Houston System

Ms. Morgan Dunn O'Connor, Chairman
Mr. Leroy L. Hermes, Vice Chairman
Mr. Raul A. Gonzalez, Secretary
Mr. Morrie K. Abramson
Mr. Michael J. Cemo
Mr. Dennis D. Golden, O.D.
Mr. Lynden B. Rose
Mr. Thad "Bo" Smith
Mr. Calvin W. Stephens

The University of Houston

Dr. Jay Gogue, Chancellor of the University of Houston System and President of the University of Houston