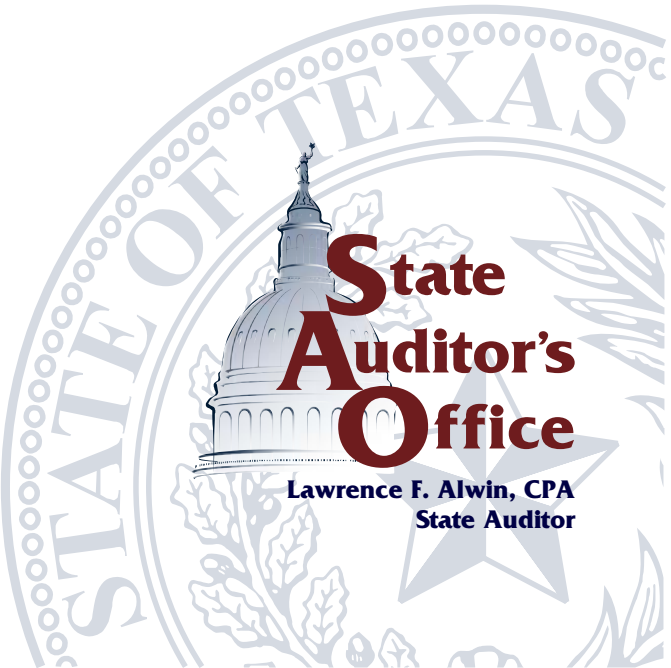
An Audit Report on

Protection of Research Data at Higher Education Institutions

June 2004

Report No. 04-035



State Auditor's Office

Lawrence F. Alwin, CPA
State Auditor

An Audit Report on

Protection of Research Data at Higher Education Institutions

SAO Report No. 04-035
June 2004

Overall Conclusion

Higher education institutions should do more to protect research data. Security of research data at the institutions we audited was inconsistent and sometimes inadequate. Although we identified instances in which research data was very well protected, we identified inconsistent security measures at each of the three institutions we audited that expose other research data to the risk of loss or misuse. This could significantly impede researchers' progress or, ultimately, result in the loss of research funding.

Background Information

We audited the protection of research data at the following institutions:

- The University of Texas at Austin (UT Austin)
- The University of Texas Southwestern Medical Center at Dallas (UT Southwestern)
- The University of Texas Health Science Center at San Antonio (UT Health Science Center)

These three institutions received more than $774 million in research funding and spent $571 million on research in fiscal year 2003. Research expenditures for Texas's public higher education institutions totaled nearly $2.2 billion during fiscal year 2003.

The institutions have ultimate responsibility for research data because they are the owners of this data and receive benefits from research such as patents, royalties, and associated funding for indirect costs. However, while institutions generally provide some degree of security to all users through perimeter firewalls or other types of network protection, they rely on decentralized departments and individual researchers to further protect research data.

Inadequate security can lead to the loss or misuse of research data, which could jeopardize institutions' reputations and their ability to achieve their missions. Although the following examples did not occur at institutions we audited, they demonstrate the importance of protecting research data:

- Not properly backing up research data has the potential to impede the progress of research. For example, Tropical Storm Allison caused the Baylor College of Medicine and the Medical School at The University of Texas Health Science Center at Houston to lose 10 years' worth of data on spinal cord injuries.

- Not securing workstations with antivirus software can leave workstations vulnerable to potential attacks, and inadequate security associated with a single workstation has the potential to have an impact on the institution's entire network. For example, in May 2004 the Sasser computer virus reportedly infected nearly one-third of the computers at The University of Texas M.D. Anderson Cancer Center and delayed some patient treatment. It is suspected that the virus entered the institution through a notebook computer.

- Because of their need for free exchange of information and open computing environments, higher education institutions in particular face a significant risk that intruders will be motivated to hack into their systems and use their extensive computing resources for unauthorized purposes. For example, hackers recently targeted and

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.

compromised TeraGrid, a network that institutions use to conduct and share research. Because of this attack, institutions that use TeraGrid took certain computers off line, which disrupted research for several days.

To minimize the risks associated with public disclosure, this report summarizes the issues we identified but does not reveal specific vulnerabilities. We provided the institutions we audited and The University of Texas System with confidential vulnerability assessments that included specific recommendations. We identified some practices being implemented at the institutions we audited that we feel are worth considering at other institutions. We have noted these as "best practices" in our report.

The institutions generally agreed with our recommendations. The institutions were already aware of the weaknesses we identified and had begun making progress and continue to make progress to address areas of concern. They have provided detailed plans for addressing their respective issues.

Key Points

Institutions should develop comprehensive information security programs for research data.

Not all of the institutions we audited have comprehensive security programs. Specifically, institutions do not always address the risk to research data in the information security policies, security risk assessments, and disaster recovery plans. Because researchers have limited guidance to follow when attempting to secure information resources, there are wide variations in security practices. In addition, none of the institutions we reviewed ensures that all users receive security awareness training to educate them on how to protect data.

Institutions should develop comprehensive protection at the user layer.

The research labs we reviewed receive varying levels of technical support. Individuals who manage information resources in these labs are researchers or instructors who may have varying levels of expertise in information security or for whom information security is not their primary responsibility. This has led to several weaknesses in data backups, antivirus software, security patches, user access, and passwords.

Institutions should develop comprehensive protection at the network and outer layers.

Each institution we audited must address specific weaknesses in its approach to network security and ensure that network equipment is properly protected. In addition, we identified unauthorized wireless access points at all of these institutions, which may expose the institutions' networks to the risk of intrusion.

Summary of Information Technology Review

We focused on the security of research data on servers and workstations in individual research labs, as well as the management of central information resources that affect research. We conducted technical vulnerability scans, but we did not attempt to exploit the vulnerabilities we identified. We also conducted wireless leakage tests in selected areas. During our audit, we identified issues that increase the risk of loss of research data, but we did not identify any specific instances in which research data had been lost or misused. We did not review administrative systems or applications such as financial, accounting, or student information systems.

Summary of Objectives, Scope, and Methodology

The objectives of the audit were to determine whether selected higher education institutions have (1) adequate controls for major research information systems to ensure that proprietary research information is sufficiently protected from loss or misuse, (2) access and security controls for the networks and information systems used for research, and (3) adequate physical security and disaster recovery plans to ensure that research information systems and data are not lost in the event of an emergency or disaster.

The scope of the audit included reviewing selected research labs' workstations and servers that contain proprietary research data and the management of central information resources that affect research.

The audit methodology consisted of interviewing staff, reviewing disaster recovery and information security plans and policies, inspecting major data centers and selected research labs, and conducting network and wireless scans to identify potential information system vulnerabilities.

Contents

Detailed Results

Appendix

Detailed Results

Introduction

Higher education institutions should do more to protect research data. Security of research data at the institutions we audited was inconsistent and sometimes inadequate. Although we identified instances in which research data was very well protected, we identified inconsistent security measures at each of the three institutions we audited that expose other research data to the risk of loss or misuse. We found that some research data is not routinely backed up or securely stored, and workstations sometimes lack current antivirus software and security patches.

The institutions have ultimate responsibility for this data because they are the owners of this data and receive benefits from research such as patents, royalties, and associated funding for indirect costs. However, while institutions generally provide some degree of security to all users through perimeter firewalls or other types of network protection, they rely on decentralized departments and individual researchers to further protect research data.

Protecting research data is important.

Inadequate security can lead to the loss or misuse of research data, which could jeopardize institutions' reputations and their ability to achieve their missions. Although the following examples did not occur at institutions we audited, they demonstrate the importance of protecting research data:

- Not properly backing up research data has the potential to impede the progress of research. For example, Tropical Storm Allison caused the Baylor College of Medicine and the Medical School at The University of Texas Health Science Center at Houston to lose 10 years' worth of data on spinal cord injuries.

- Not securing workstations with antivirus software can leave workstations vulnerable to potential attacks, and inadequate security associated with a single workstation has the potential to have an impact on the institution's entire network. For example, in May 2004 the Sasser computer virus reportedly infected nearly one-third of the computers at The University of Texas M.D. Anderson Cancer Center and delayed some patient treatment. It is suspected that the virus entered the institution through a notebook computer.

- Because of their need for free exchange of information and open computing environments, higher education institutions in particular face a significant risk that intruders will be motivated to hack into their systems and use their extensive computing resources for unauthorized purposes. For example, hackers recently targeted and compromised TeraGrid, a network that institutions use to conduct and share research. Because of this attack, institutions that use TeraGrid took certain computers off line, which disrupted research for several days.

Weaknesses in the protection of research data also could result in the loss of research funding, which is a key source of institutions' funding. The three institutions we audited received more than $774 million in research funding during fiscal year 2003,

an increase of $37 million since fiscal year 2002. These institutions also received more than $18 million in revenue from patent royalties and equity in start-up companies in fiscal year 2003.

The benefits of Texas higher education institutions' research efforts are not limited to the institutions themselves. The commercialization of intellectual property that institutions create from their research can drive the development of start-up businesses and new industries across the state. The Comptroller of Public Accounts estimates that every $1 spent from federal and out-of-state funded research results in a $3.32 impact on the Texas economy. In addition to its effect on the economy, research that higher education institutions conduct can directly affect the welfare of Texas citizens through medical discoveries.

Institutions we audited are conducting critical research.

We audited The University of Texas at Austin (UT Austin), The University of Texas Southwestern Medical Center at Dallas (UT Southwestern), and The University of Texas Health Science Center at San Antonio (UT Health Science Center). Specifically, we audited these institutions' central information technology services, which provide basic connectivity for researchers. In addition, we audited several research labs and departments at each institution that are conducting critical research in areas such as cancer and alternative sources of energy. Table 1 describes research at the institutions we audited.

Table 1

Summary of Research at the Institutions We Audited

Institution	Research Funding in Fiscal Year 2003 (in millions)	Research Expenditures in Fiscal Year 2003 (in millions)	Revenue from Institution Research in Fiscal Year 2003 (in millions)	Number of Current Research Projects
The University of Texas at Austin	$381	$185	$3.9	3,500
The University of Texas Southwestern Medical Center at Dallas	$225	$280	$10.9	2,000
The University of Texas Health Science Center at San Antonio	$168	$106	$3.8	3,900

Source: Unaudited data from each institution

Research is generally conducted in decentralized, open computing environments.

Many higher education institutions have established open computing environments to facilitate the free exchange of information. In addition, research has historically been conducted in a decentralized fashion in individual research departments and labs. While this approach enables data to move freely, it provides minimal security functionality, impairs an institution's ability to implement and enforce standard security measures, and shifts primary responsibility for information security to individual users at the lab or department level.

Institutions generally provide some degree of information technology security for the entire institution through security policies, firewalls, and other network security measures; however, they generally do not provide additional security measures for research data. Moreover, some research labs may choose not to use the security features the institutions provide.

Although researchers are responsible for ensuring the security of research data, information security may not be their area of expertise. Researchers also may not be aware that their research data needs a higher level of protection. In a recent discussion on institutions' role in economic development, The University of Texas System (System) chancellor noted that researchers may not always recognize that the research they are conducting has market merit.

Institutions should use a defense-in-depth strategy to protect information resources.

In open computing environments, it is important that institutions take the necessary steps to secure their information resources. This can be done by implementing a "defense-in-depth" strategy—using multiple layers of security while still maintaining the free flow of information desired in an academic and research setting. The concept of the defense-in-depth strategy is to not rely on any single type of protection but to provide different types of protection at different layers within the institution.

Best Practice: Defense-in-Depth Strategy

One lab we reviewed at UT Austin uses several different layers of firewalls and security depending on the sensitivity of data. It also isolates its Windows computers from research data stored inside the protected firewall zone. In addition, this lab established its own security policies.

One model of the defense-in-depth strategy is composed of three different levels to provide protection at the user, network, and outer layers:

- **User layer.** The user (or innermost) layer is where the research data resides. The user is ultimately responsible for this data, and the adequacy of protection at the level is directly affected by the user's knowledge of information security and the direct support that the user receives from technical security staff. Within the user layer, the user and technical support staff are responsible for making regular data backups, properly patching and securing the operating system, properly updating antivirus software, and correctly configuring firewalls.

- **Network layer.** The network layer includes security measures such as enterprisewide antivirus products for e-mail and file servers, an enterprisewide security patch management service, internal scanning of servers and critical infrastructure, a perimeter firewall, and an intrusion detection system.

- **Outer layer.** The outer layer protects against external intrusion. Protection at this layer can be significantly enhanced through the use of a managed monitoring service that can provide rapid notification of trends and inappropriate activities involving an institution's network. This layer also encompasses protection of remote and wireless access to the institution's network.

An institution's security policies cover all three layers of protection and are crucial to ensuring that each layer is functioning properly. In addition, the technical support received at each of these layers is critical. It is essential that institutions implement all elements of the defense-in-depth strategy to adequately protect research data. The

institutions we audited have not fully implemented comprehensive defense-in-depth strategies. At all of the institutions we audited, we identified various degrees of weaknesses or vulnerabilities at the user layer in data backups, antivirus software, security patches, user access, and passwords. We also identified weaknesses or vulnerabilities at the network and outer layers in areas such as perimeter security, network monitoring, and intrusion detection.

Chapter 1

Institutions Should Develop Comprehensive Information Security Programs for Research Data

Not all of the institutions we audited have comprehensive security programs to ensure that research data is adequately protected. In addition, none of the institutions we audited ensures that all users receive ongoing security awareness training that educates them on how to protect data.

The research labs we reviewed also receive varying levels of technical support. Individuals who manage information resources in these labs are researchers or instructors who may have varying levels of expertise in information security or for whom information security is not their primary responsibility. This has led to several weaknesses in data backups, antivirus software, security patches, user access, and passwords.

Chapter 1-A

Institutions Do Not Always Have Comprehensive Security Programs

Not all of the institutions we audited have comprehensive security programs. Specifically, institutions do not always address the risk to research data in their information security policies, security risk assessments, and disaster recovery plans. UT Southwestern and the UT Health Science Center have comprehensive policies, but none of the institutions we audited provides specific guidance to researchers on how to protect valuable research data. While institutions we audited provide researchers with general procedures for conducting research, this guidance does not include specific information on protecting research data. Because researchers have limited guidance to follow when attempting to secure information resources, there are wide variations in security practices. In addition, the absence of approved policies makes the enforcement of information security across departments difficult and leaves institutions unable to hold users of information resources accountable for complying with security policies.

Selected Texas Administrative Code Requirements

The Texas Administrative Code, Title 1, Chapter 202, requires state entities to:

- Establish information security policies in numerous areas.
- Maintain a written disaster recovery plan for information resources.
- Maintain a business continuity plan that covers all business functions. The plan should include a security risk assessment to weigh the cost of implementing preventive measures against the risk of loss from not taking action.

In the absence of institutionwide policies, some research labs we reviewed have established their own information security policies. For example, two labs we reviewed at UT Austin have established policies in areas such as minimum password length, network security, and account access. One of these labs has established additional security policies, in part because the sponsors of its classified research require it to implement extra security measures.

Institutions do not include research in their institutionwide risk assessments and disaster recovery plans.

Although the institutions we audited have conducted high-level risk assessments of their information resources, none of them includes research in their overall, institutionwide risk assessments. Because research is part of the institutions' missions, it should be addressed in their risk assessments. In addition, the institutions we audited do not fully address research information and systems in their disaster

recovery plans. Although institutions are required to develop disaster recovery plans for information resources, individual labs are not always required to do so. However, even though the three institutions did not include research in their disaster recovery plans, the labs we reviewed had not developed their own disaster recovery plans. Risk assessments and disaster recovery plans are important in ensuring that institutions weigh the cost of implementing preventive measures against the risk of loss.

Recommendations

Institutions should:

- Develop, implement, and enforce all information security policies required by the Texas Administrative Code.
- Conduct comprehensive risk assessments of significant research data and systems that (1) include a cost-benefit analysis to ensure that the expense of security safeguards is commensurate with the value of the assets being protected and (2) weigh the cost of implementing preventive measures against the risk of loss from not taking action.
- Determine how to incorporate critical or high-value research information resources into disaster recovery plans, either by explicitly addressing these research information resources in the overall disaster recovery plans or by coordinating the development of plans for individual research labs to complement their overall plans.

Chapter 1-B

Institutions Do Not Always Provide Researchers with Information Security Training

None of the institutions we reviewed ensures that all users receive ongoing security awareness training (as required by the Texas Administrative Code) that educates them on their information security responsibilities. While providing training to all users can be a difficult task, security awareness training is essential to ensure that users are aware of how to protect their data.

Although the institutions offer limited security awareness training during new employee or student orientations or for certain groups of users, not all users attend this training. For example, the UT Health Science Center's Information Security Office provides information security training to dental students during the Dental School orientation, but other students do not receive security training. Ensuring that all students receive security training is important because many students participate in research efforts.

The UT Health Science Center and UT Southwestern provide staff with periodic updates to security training through videotapes or Web-based training. However, the UT Health Science Center requires most staff (but not all staff) to attend the periodic updates and, at the time of our audit, UT Southwestern had not made information technology training available to staff during the past nine months. Although UT Austin provides security awareness training to some students and new employees, it

has not established ongoing security awareness training for all users as required by the Texas Administrative Code.

None of the institutions has fully implemented a security agreement and log-on banners.

The institutions we audited were not complying with the System's policy to require users to periodically sign security agreements asserting that they will comply with information security policies. The Texas Administrative Code also requires that all authorized users of information resources (including temporary employees and employees of independent contractors) formally acknowledge that they will comply with the security policies and procedures in order to be granted access to information resources.

UT Southwestern requires all faculty, employee, temporary employee, contractor, and student users of its information resources to sign security agreements every year, but it does not manage this process to ensure that these individuals keep their agreements up to date. The UT Health Science Center requires staff to sign a form during orientation acknowledging that they understand UT Health Science Center policies, including information security requirements. However, it does not require students and temporary and contract staff who have access to information resources to sign security agreements. UT Austin requires some users to sign security agreements to get access to sensitive applications. However, not all students who conduct research are required to sign this agreement.

Although some labs we reviewed displayed an initial log-on banner showing a warning against unauthorized use and reminding users of their information security responsibilities, these banners were not used consistently at any institution we audited. The Texas Administrative Code requires that state entities use log-on security banners.

Recommendations

Institutions should:

- Develop and implement required information security awareness training for all users that creates an understanding of (1) the security threats and vulnerabilities to which the institution is exposed and (2) the measures that can be taken to address these threats, including backups, the use of antivirus software and personal firewalls, and security patches.

- Comply with Texas Administrative Code requirements that all users acknowledge their understanding of information security requirements and determine how often users should re-execute this acknowledgement to maintain access to information resources.

- Implement security banners, required by the Texas Administrative Code, that are displayed when users access networks and applications.

Chapter 1-C

Institutions Do Not Always Provide Information Technology Support to Researchers

Researchers implement some of their own information security or depend on their academic departments for information technology support. As a result, the labs we reviewed receive varying levels of support. Some of the individuals who manage information resources in the labs we reviewed are researchers or instructors who have varying levels of expertise in information security or for whom information security is not a primary responsibility. Labs may leave management of workstations up to the individual members of the research staff working in the labs. This has led to several weaknesses in data backups, antivirus software, security patches, user access, and passwords.

Researchers who do not already have or do not hire staff with information technology expertise rely on their academic departments for information technology support. While some departments have staff dedicated to providing information technology support at the department level, these individuals do not always provide information technology support to research labs in their departments. For these labs, the adequacy of the security of research data is directly dependent on the information technology expertise of the individual researcher or lab administrator.

Best Practice: The UT Health Science Center's Technical Service Representative Program

The UT Health Science Center requires that each department have at least one designated technical service representative (TSR) appointed by the respective dean, director, or chair. The TSR program was designed to enable each department to have at least one computing technology point of contact with responsibility for first-line problem diagnosis and resolution of technical questions.

Only one institution we audited—the UT Health Science Center—requires each department to designate individuals to provide technical support to the departments or serve as primary contacts to receive information on technology issues (such as virus alerts or the need to install security patches) that require immediate action (see text box for additional details). Some UT Austin departments have appointed technical support coordinators to provide information technology support; however, neither UT Austin nor UT Southwestern requires all departments to appoint technical support staff.

Although some departments have technical support staff, these individuals are not always properly trained and qualified. Some technical support staff members are trained system administrators, but some are simply individuals who work in the department. In addition, these technical support staff may not offer support to the labs or have the authority, staff, or time to manage all workstations. To ensure that system administrators meet minimum qualifications, the UT Health Science Center has developed a program to train system administrators to properly secure the systems used in their departments, but it has not yet implemented this program.

Recommendations

Institutions should:

- Consider requiring departments to designate individuals to provide technical support to the departments and labs and to serve as primary contacts to receive information on technology issues that require immediate action.

- Identify the minimum qualifications that individuals who provide technical support should have and provide training to ensure that they possess these qualifications.

- Ensure that the technical support representatives have responsibility for the security of all department and lab workstations and servers (including personal workstations) that use the institution's network.

Institutions Should Develop Comprehensive Protection at the User Layer

The institutions we audited leave security over the innermost layer of information systems up to users (researchers or research staff) and their technical support, if any. As a result, there is inconsistent protection of research data among research labs. The user interacts directly with the data and is responsible for the first level of protection. Because of this, it is essential that users receive security awareness training and have good technical support and security policies to provide them with specific guidance. However, as discussed in Chapter 1, none of the institutions we audited has provided comprehensive user training and technical support for all researchers. Although we identified instances in which research labs were protecting research data very well, we also found instances in which research data was not protected. Specifically:

- Research data stored on workstations is not always backed up to provide timely resumption of research activities. Research data that is stored on a server is more likely to be backed up, but the backup tapes are not always stored in a secure location. In addition, there is not always adequate physical security to prevent loss of research data.

- Workstations in research labs do not always have up-to-date antivirus software or properly configured firewall software on all workstations. Research labs do not always secure their operating systems by applying security patches.

- Research data is not always protected with proper password policies and access controls.

Chapter 2-A

Research Labs Have Inconsistent Backup Processes

The research labs we reviewed do not always have adequate backup procedures to provide timely resumption of research activities or adequate physical security to prevent loss of research data. This increases the risk that research data will be lost, which could significantly impede researchers' progress or, ultimately, result in the loss of grant funding. While some institutions and academic departments may offer space for researchers to store data, the space offered is either limited or, according to research staff, too expensive. Providing centrally managed servers on which researchers can store data is not without costs; however, storing data in this manner could offer more protection because data could be backed up regularly and the backup tapes could be stored off-site.

UT Southwestern is the only institution we audited that has policies requiring researchers to back up data stored on workstations. None of the other institutions we audited provides researchers with guidance on how to perform backups.

The research labs we reviewed have inconsistent backup procedures and do not always back up data or store backup tapes in secure locations.

Researchers and staff in the labs we reviewed store some or all of their research data on workstations. Other labs we reviewed conduct most of their work on workstations but move the data to a central server or archive the data after work is complete.

Individuals who store research data only on workstations are responsible for performing regular backups of this data. While some researchers back up their data on a regular basis, others back up their data too infrequently. In some of the labs we reviewed, researchers back up their data anywhere from once a month to once every six months. As a result, these researchers could lose from one to six months of work if something happened to their workstations. Other researchers do not back up their data at all.

When labs use central servers to store data, they generally have strong backup practices because they back up data on these servers on a daily basis. However, they do not always store the backup tapes in secure locations. For example, several of the research labs we reviewed store their backup tapes in the same location as their servers, which could significantly hinder recovery capabilities in the event of a disaster. Although some research labs have a fireproof safe at the facility in which they can store backups, others do not.

Backups are important because many research labs' workstations and servers are located in labs that have a higher-than-normal exposure to environmental hazards. For example, workstations can be located in labs that use chemicals and natural gas as part of research experiments. In addition, workstations and servers are located in offices and labs that may be unlocked during the day, which increases the risk of potential theft or damage to computer equipment containing research data. Some of the labs we reviewed require staff to lock the doors when labs are unattended or limit access through key cards. However, other labs leave their doors open when they are unattended, even though some of them are located on high-traffic corridors. Research labs have experienced problems with theft in the past. For example, two research labs we reviewed reported the theft of laptop computers during the past year.

Recommendations

Institutions should:

- Require all researchers to perform regular backups of research data. In addition, they should provide specific guidelines for researchers regarding the creation and storage of backup tapes. The guidelines should consider the confidentiality and value of the data, as well as any potential threats that could lead to the loss of data.

- Consider providing an institutionwide backup capability, including central servers for backups and central storage for backup media.

- Ensure that workstations and servers in departments and labs are protected from environmental hazards and theft.

Chapter 2-B

Research Labs Do Not Always Install and Update Antivirus Software, Security Patches, and Personal Firewalls

The workstations and servers in the research labs we reviewed do not always have the most current antivirus and personal firewall software and up-to-date security patches to protect research data from unauthorized access or destruction. Properly

updated and configured antivirus and personal firewall software helps to block intruders, viruses, worms, and other unwanted applications. However, old or improperly configured antivirus and personal firewall software makes workstations (and any data on the workstations) more susceptible to unauthorized access and could possibly compromise other resources on the main network.

Not all researchers have up-to-date antivirus and personal firewall software.

All three institutions we audited offer antivirus software to users, and two offered it for home use. However, because researchers may manage their own workstations, they are responsible for installing and updating antivirus software. As a result, the management of antivirus software in research labs is inconsistent. In addition, the antivirus software that institutions offer to users does not always work on all workstation operating systems. Further, some workstations that require specific operating systems to run equipment do not have antivirus or firewall software because such software interferes with the application running the equipment.

At the time of our audit, the institutions we audited did not have centralized antivirus servers to "push" updates of antivirus software to all individual workstations to ensure that all users have antivirus software with the most current antivirus definitions. Instead, the institutions used other methods of providing virus alerts and updates such as posting them on their Web sites and sending e-mail notifications. However, they still rely on users to update their antivirus definitions. Having users update their computers in a timely manner is important because viruses and worms can spread quickly in an open environment.

Antivirus and Personal Firewall Software

Antivirus software provides protection against viruses and malicious code (such as worms and Trojan horses) by detecting and removing the malicious code and by preventing unwanted effects.

Personal firewalls control access to and from a computer by filtering network traffic and allowing only authorized communications.

Source: *Information Security: Technologies to Secure Federal Systems*, U.S. General Accounting Office Report 04-467, March 2004.

Only one of the institutions we audited offers users personal firewall software, and none of the institutions we audited requires users to install personal firewall software on individual workstations. Personal firewalls are an important added protection, particularly in an open academic environment, and are critical in protecting research workstations and data against viruses and attacks by hackers.

Researchers do not always install up-to-date security patches on their workstations and servers.

As with antivirus software, research lab workstations and servers do not always have up-to-date security patches, which increases the vulnerability of these devices to attacks from both inside and outside the network. None of the institutions we audited has an automated system to "push" security patches to all users or notify all users of the existence of these patches. Some research labs we reviewed configure newer versions of Windows operating systems to automatically download and install security patches; however, technical support staff or users must manually update all other versions of operating systems when security patches for those operating systems become available.

Our technical scans identified critical vulnerabilities that indicate that not all users in research labs are installing security patches. Specifically, the scans identified vulnerabilities that can be fixed by installing the most current available security

patches. In addition, some of these vulnerabilities could be eliminated if workstations were properly configured and unnecessary services were turned off.

Some of the vulnerabilities we identified increase the risk that an attack could result in an unauthorized individual gaining system-level privileges or the ability to access data, which could result in an unauthorized disclosure or destruction of research data. A compromised workstation could also serve as an intermediate point for launching additional attacks on a lab's network and on an institution's main network.

Recommendations

Institutions should:

- Where possible, develop, implement, and enforce policies on antivirus and firewall software, including polices to require that all workstations and servers connected to the main campus network have current firewall and antivirus software.

- Provide researchers with training and specific recommendations for the levels of antivirus and firewall protection needed to secure different classifications of research data based on the value of the data, as well as potential threats and the likelihood of their occurrence.

- Consider limiting access to or segregating devices with older operating systems that cannot be protected with antivirus and firewall software from the network.

- Develop, implement, and enforce institutionwide policies on security patch management and associated installation schedules that take into account the relative importance of various systems.

- Improve the process to notify labs about security patches and provide training to lab staff on how to implement security patches.

- Ensure that research labs install and operate current security patches on all servers, workstations, and personal laptop computers. This could be done by implementing an automated security patching process on the central, department, or lab networks.

Chapter 2-C

Research Labs Do Not Always Adequately Limit Access to Research Data

The research labs we reviewed do not always follow adequate procedures for preventing attempts from unauthorized users to access their data. In addition, they do not always have adequate password policies. This increases the risk that unauthorized individuals could access research data.

We identified instances in which users at both UT Southwestern and the UT Health Science Center had their workstations configured to allow the sharing of data on their hard drives across the network. This is a violation of both institutions' policies. We identified similar instances at UT Austin; however, UT Austin does not have policies

to discourage users from sharing data on their individual workstation hard drives or to instruct them on how to share this data securely. UT Austin does provide guidance for securing desktop file sharing on its main information security Web site. If users have enabled sharing of their resources, other users on the network can potentially see and attempt to access those resources. Some researchers may have a legitimate need to share data on their workstation hard drives, but access to these files should be limited through passwords or other restrictions.

The research departments and labs we reviewed do not always have adequate password policies.

The research labs we reviewed do not always have adequate password policies for their servers and workstations. The following password weaknesses create significant risks that unauthorized users could gain access to research data, servers, and workstations:

- Research labs we reviewed do not always have adequate minimum password lengths (some passwords were six or fewer characters or were blank), and they do not always have password requirements that follow the Department of Information Resources' guidance regarding maintenance of password history, how long passwords must be used before they can be changed, and the complexity of password composition.

- Research labs we reviewed do not always require users to change their passwords or ensure that passwords eventually expire. For example, one lab we reviewed never changed the administrator password on its server from the default password, which could give an unauthorized user full control over the server. It is common for hackers to know, share, and exploit default passwords for many operating systems and applications.

- Common-area workstations in research labs generally do not require passwords, and users may not need passwords to log on to their individual workstations. Further access to databases, however, generally requires a password.

Our technical scans also identified workstations for which one or more user accounts do not require passwords. This exposes these workstations and any research data they contain to unauthorized access. Many other workstations have administrator accounts with blank passwords. This vulnerability could give a hacker full control of those servers or workstations and, if those devices share files, could enable the hacker to access other servers.

The research labs we reviewed do not always enable features that protect against unauthorized access attempts.

The research labs we reviewed do not always enable software features that help prevent unauthorized access to their servers by limiting the number of unsuccessful access attempts. This is important, especially given the weaknesses in password controls discussed above. As a result, repeated attempts by intruders to gain unauthorized access could go undetected. In addition, some labs allow users to log on to servers simultaneously from multiple workstations.

The absence of a forced log-off and allowing multiple log-ons increase the risk that an unauthorized user could gain access to research data when research personnel do

not log off or use password-protected screen savers when they are away from their workstations, where possible. Research labs' automated security logs would not detect this type of unauthorized access because the user would appear to be authorized. Furthermore, although automated security logs capture information such as access attempts, successful log-ons, and processing errors, individuals who manage research lab servers do not consistently examine those logs. While some labs we reviewed examine their security logs on a daily basis, other labs examine their security logs on a weekly or monthly basis, and some of them do not review these logs at all. Reviewing security logs on a regular basis is important because logs can reveal unauthorized attempts to access data.

In addition, we identified unattended workstations in research labs that are not automatically logged off or timed-out because experiments may be running continuously on these workstations. Normally, this risk could be mitigated through the use of password-protected screen savers. However, such screen savers are not consistently used on workstations and, in some cases, cannot be used because they interfere with special applications. It is typically up to the user to activate these screen savers.

Recommendations

Institutions should:

- Establish and enforce a policy regarding sharing data stored on individual workstation hard drives. If users are permitted to share data on their hard drives, institutions should instruct them on how to share this data securely. Institutions should also consider conducting regular scans to identify instances in which users are sharing their hard drives to monitor compliance with established policies.

- Ensure that users are made aware of the importance of securing their workstations and servers by changing default accounts and ensuring that all accounts have passwords.

- Where possible, ensure that password policies for research departments are strengthened to follow the Department of Information Resources' guidelines for length, complexity, reuse, and aging.

- Ensure that server administrators review security logs.

- Where possible and appropriate, ensure that workstations use password-protected screen savers when users are away from their workstations.

Institutions Should Develop Comprehensive Protection at the Network and Outer Layers

The institutions we audited have varying levels of network security in place and protect their perimeters and main networks using different approaches. Each institution must address specific weaknesses in these approaches and ensure that network equipment is properly protected from environmental hazards. In addition, none of the institutions we audited monitors its internal network traffic for indications of unauthorized access by internal users.

All institutions we audited allow users to access their main networks using wireless devices, and we identified unauthorized wireless access points at each institution. Unauthorized access points may expose the institutions' networks to the risk of intrusion.

Chapter 3-A

Institutions Do Not Always Provide a Secure Environment on Their Main Networks for Researchers to Use

The protection of an institution's main networks is critical to preventing unauthorized access from both inside and outside the institution. The three institutions we audited protect their perimeters and main network using different approaches. Specifically:

Perimeter Security Controls

The Texas Administrative Code requires that each agency head or his/her designated representative and information security officer establish a perimeter protection strategy to include some or all of the following components based on the agency's security risk management decisions:

- Demilitarized Zone (DMZ)
- Firewall
- Intrusion Detection System
- Router

Source: Texas Administrative Code, Title 1, Section 202.7(i)

- Both UT Southwestern and the UT Health Science Center have border firewalls configured to block traffic to specific communication ports. In contrast, UT Austin has chosen to perform filtering by using routers instead of a border firewall. UT Austin reports that there is no firewall equipment capable of properly performing in the UT Austin network operations environment. UT Austin relies on individual departments to secure their respective information resources.

- Both UT Southwestern and the UT Health Science Center have demilitarized zones (DMZ) intended to limit outside users from obtaining direct access behind the firewall. However, neither institution has moved all public services to the DMZ. Because UT Austin performs filtering by using routers instead of a border firewall, it has not implemented an enterprise DMZ to isolate all publicly accessed servers. UT Austin relies on individual departments to consider protections for their publicly accessed servers.

- All three institutions we audited have some form of intrusion detection systems to identify potential security incidents. UT Southwestern uses commercial intrusion detection software. UT Austin performs some monitoring of its information systems using custom tools developed by its staff and monitors its main network to identify nonfunctioning devices, excessive bandwidth usage, and abnormal traffic patterns. UT Austin also reports that it plans to purchase an intrusion detection system in the future. The UT Health Science Center contracts out for continuous intrusion detection services to identify potential security

incidents. The UT Health Science Center' contractor can also use the information it obtains from analyzing traffic on its other clients' networks to provide early warnings to the UT Health Science Center before it is affected by a security incident.

Best Practice: The UT Health Science Center's Use of TeleWall

The UT Health Science Center uses TeleWall to log all calls through its PBX system, including calls via fax and modem. TeleWall blocks incoming fax calls without caller ID to certain fax lines and plans to use it to block unauthorized modems. In addition, certain events—such as an internal user dialing an outside Internet service provider—trigger an e-mail to alert the UT Health Science Center's Information Security staff so it can take appropriate follow-up action.

- All three institutions we audited conduct periodic network scanning to identify vulnerabilities.
- The Health Science Center uses software to log and filter all analog calls via fax and modem (see text box).

We also found that institutions do not always protect critical network equipment from physical dangers and theft. Specifically, at UT Austin and UT Southwestern, we found significant physical and environmental security weaknesses over critical network components that provide connectivity to their campus users (including researchers) and other users of their networks.

The institutions we audited do not monitor internal network traffic.

None of the three institutions we audited monitors internal traffic. This is significant because many security incidents stem from internal users' unintentionally downloading viruses from their personal Internet-based e-mail (such as Hotmail or Yahoo! mail).

Recommendations

Institutions should:

- Ensure that they secure their network perimeters by using components such as DMZs, firewalls, intrusion detection systems, and routers.
- Periodically conduct vulnerability scans of their networks and monitor internal network traffic for unusual activity that could indicate unauthorized internal user actions or viruses.
- Ensure that critical network equipment is protected from physical dangers and theft.

Chapter 3-B

Institutions Do Not Always Ensure that Wireless Network Access Is Secure

All institutions we audited have wireless access. While UT Southwestern's and the UT Health Science Center's overall implementation of wireless access points is relatively secure, we identified unauthorized wireless access points at all three institutions we audited. These unauthorized access points may expose the institutions' networks to the risk of intrusion. In addition, UT Austin does not perform regular monitoring of its wireless network for unauthorized wireless access points; as a result, we identified a large number of unauthorized access points at that

institution. Some of these unauthorized access points may appear to be authorized because of the access points' configuration settings.

The UT Health Science Center's and UT Southwestern's wireless networks require users to use virtual private network client software to access campus network resources from the wireless network. As an additional precaution, the UT Health Science Center requires users that have wireless access to register their wireless laptops or other devices to limit access to only UT Health Science Center users.

UT Austin's goal in providing wireless services is to provide network access at various points across the campus. Affiliated wireless users, primarily students and faculty, are redirected automatically to the Public Network Authentication System, where they must log in using their UT Austin user account identification numbers before they connect to the campus network. This helps to prevent unauthorized access to authorized wireless access points. However, unlike UT Southwestern and the UT Health Science Center, after an individual logs on to UT Austin's wireless network, the data transmitted is not encrypted unless the individual uses an application that encrypts the data.

Recommendations

Institutions should:

- Implement and enforce policies for wireless access on campus, including a policy that prohibits unauthorized wireless access points.
- Implement monitoring procedures to detect and locate unauthorized wireless access points. This could be done by implementing some form of autosensing device for their wireless networks.
- Require users who transmit confidential or sensitive data on the wireless network to use encryption mechanisms.
- Ensure that users understand the risks of transmitting data on a wireless network through security awareness training or guidelines.

Appendix

Objectives, Scope, and Methodology

Objectives

The objectives of the audit were to determine whether selected higher education institutions:

- Have adequate controls for their major research information systems to ensure that proprietary research information is sufficiently protected from loss or misuse.
- Have access and security controls for the networks and information systems used for research.
- Have adequate physical security and disaster recovery plans to ensure that research information systems and data are not lost in the event of an emergency or disaster.

Scope

We audited the following institutions:

- The University of Texas Health Science Center at San Antonio (UT Health Science Center)
- The University of Texas Southwestern Medical Center at Dallas (UT Southwestern)
- The University of Texas at Austin (UT Austin)

At each institution, the scope of the audit included reviewing (1) selected research labs' workstations and servers that contain proprietary research data and (2) the management of central information resources that affect research.

Methodology

The audit methodology consisted of interviewing staff, reviewing disaster recovery and information security plans and policies, inspecting major data centers and selected research labs, and conducting network and wireless scans to identify potential information system vulnerabilities.

Information collected included the following:

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

- Lists of institution employees and terminations and selected research labs' user populations

Procedures and tests conducted included the following:

- Interviews with key staff regarding 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' Internet Scanner, BindView's bv-Control for Windows, and bv-Control for Netware scanning tools
- Limited wireless leakage tests using Netstumbler and AeroPeak
- Sampling of selected research lab workstations and servers to test user access controls

Information resources reviewed included the following:

- Access and security controls for the centrally managed network and information systems that store research data
- Disaster recovery plans for the general centrally managed network and information systems that store research data
- Physical security controls protecting the centrally managed network and research information systems that store research data

Criteria used included the following:

- Texas Administrative Code, Title 1, Chapter 202 (Information Security Standards)
- Department of Information Resources' Business Continuity Planning Guidelines
- Control Objectives for Information and related Technology (COBIT), Information Systems Audit and Control Association
- Best practices from a variety of sources including the U.S. General Accounting Office, the SANS Institute, and EDUCAUSE

Other Information

We conducted fieldwork from January 2004 through April 2004. This audit was conducted in accordance with generally accepted government auditing standards applicable to performance audits.

The following members of the State Auditor's staff performed the audit work:

- Paige Buechley, MBA, MPAFF, CIA, CISA (Project Manager)
- David Dowden

- Dean Duan, CISA (Information Systems Audit Team)
- Vicki Durham, MBA
- Natasha Kelly, MBA
- Steve Sizemore, CGAP, CIA, CISA (Information Systems Audit Team)
- Sarah Slaughter, CPA
- Michael Yokie, CISA (Information Systems Audit Team)
- Chuck Dunlap, 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

The University of Texas System Board of Regents

Mr. James Richard Huffines, Chairman
Mrs. Rita C. Clements, Vice-Chairman
Mr. Woody L. Hunt, Vice-Chairman
The Honorable Cyndi Taylor Krier, Vice-Chairman
Mr. John W. Barnhill, Jr.
Mr. H. Scott Caven, Jr.
Ms. Judith L. Craven, M.D., M.P.H.
Mr. Robert A. Estrada
Mr. Charles Miller

The University of Texas System

Mr. Mark G. Yudoff, Chancellor

The University of Texas at Austin

Dr. Larry R. Faulkner, President

The University of Texas Southwestern Medical Center at Dallas

Dr. Kern Wildenthal, President

The University of Texas Health Science Center at San Antonio

Dr. Francisco G. Cigarroa, President