An Audit Report on

Security of Confidential Electronic Information at Selected Health and Human Services Agencies

February 2003

Report No. 03-017

State Auditor's Office

Lawrence F. Alwin, CPA
State Auditor

An Audit Report on

Security of Confidential Electronic Information at Selected Health and Human Services Agencies

SAO Report No. 03-017
February 2003

Overall Conclusion

Confidential Information

Confidential information is information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

Source: Texas Administrative Code for Information Security, 202.1 (3)

Some Texas health and human services agencies do not adequately protect the confidential client information in their automated systems. Numerous weaknesses in external and internal controls could allow individuals inside and outside these agencies to gain unauthorized access to automated systems and read, copy, modify, or delete confidential client information. This lack of protection is especially serious because all health and human services agencies are on a consolidated network. Without proper network security measures, any employee or contractor of any agency on the network could potentially access confidential information of other agencies on the network. Each agency reviewed has this weakness.

In addition, the agencies we reviewed lack effective security management programs, which are essential to ensure the cost-effective use of security resources. The agencies have not classified data, assigned data ownership, or determined the resources necessary to secure their data. Without such a program, these agencies may not correctly allocate funds for data security or may not appropriately spend these funds.

All of the issues we identified in this audit are violations of the Texas Administrative Code (TAC) (Title 1, Section 202) for Information Security. TAC 202, revised in June 2002, represents current requirements as well as best practices for information security.

Health and human services agencies' information systems contain highly confidential data relating to physical and mental health, child abuse and neglect, the elderly, Medicaid and Medicare, drug and alcohol abuse, physical and mental disability, and children's health insurance. By not protecting their information, these agencies risk losing the public's confidence and being unable to serve their clients. They also open themselves up to financial losses if they violate federal or state law, if they have to re-create lost data, or if they are sued because of a breach of privacy.

This report contains a general summary of the network security, system access, and TAC compliance issues we identified at selected health and human services agencies. To minimize the risk of public exposure, this report does not include the names of the agencies we audited or identify specific vulnerabilities that could allow someone to exploit their systems. We provided the audited agencies with detailed information regarding the specific vulnerabilities we identified as well as our recommendations for improvements.

Cost and organizational support can hamper security improvements. We understand that cost may be an issue given the current state budget projections. However, the significance of the risk that confidential information will be disclosed requires management to carefully assess the cost-benefit of effectively managing that risk. A few of our recommendations require additional hardware. For agencies of this size, the required hardware is inherently

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

This audit was conducted in accordance with generally accepted government auditing standards.

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

expensive. Wherever possible, we identified interim solutions that can be implemented until the necessary hardware can be obtained. The majority of our recommendations require staff members' time and/or management's commitment to developing and complying with policies and procedures.

Summary of Management's Response

The agencies we audited generally agree with our recommendations. They have provided detailed plans, time lines, and names of individuals or units responsible for addressing each recommendation.

Summary of Information Technology Review

This audit was limited to selected information systems that contain confidential client information. We also reviewed the perimeter security and network controls that authenticate users and allow general access to the agencies' internal networks, e-mail, and the Internet. We did not examine the accuracy of the data in any agency systems or review the controls over any other systems such as the financial or human resources systems. In addition, we examined the physical security over the agencies' computer equipment and reviewed the disaster recovery plans for the selected systems.

We conducted network scans at the selected agencies to identify vulnerabilities in the networks that housed the systems we audited. We used Internet Security Systems' Internet Scanner™ to scan agreed-upon network areas. These areas did not cover all of the agencies' networks. We also used the Bindview™ scanning tool to confirm our findings in the area of access controls. In addition, we performed wireless leakage tests at selected locations.

Detailed Results

Introduction

Health and human services agencies deliver various services to clients across the state. In doing this, they generate, collect, and/or maintain confidential client information such as social histories, criminal histories, medical records, financial information, social security numbers, and billing records. The fact that these agencies have regional and field offices where data is stored and accessed further complicates their information security.

Texas's health and human services agencies, along with a few other agencies and multiple public and private entities (see text box on page 2), make up the Health and Human Services Consolidated Network (HHSCN). Together, the health and human services agencies employ 33.8 percent of the State's approximately 143,000 employees, so a large number of people have access to tremendous amounts of decentralized, confidential data. In addition, numerous outside contractors and service providers such as hospitals and university medical institutions have access to this network. When coupled with the types of poor controls over user and provider access we found, the number of people with access greatly increases the risk that this data could be misused, lost, or stolen.

Federal and state agencies are facing increased demands to protect confidential information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established specific requirements for protecting health information from unauthorized use or disclosure. In addition, Senate Bill 11, passed during the 77th Legislative Session, specifies the use and disclosure of protected health information. By not protecting their information, these agencies risk losing the public's confidence and being unable to serve their clients. They also open themselves up to financial losses if they violate federal or state law, if they have to re-create and resecure lost data, or if they are sued because of a privacy breach.

The following examples demonstrate what can happen when confidential information is inadequately secured:

- Because of poor access controls, a Department of Health customer service representative was able to access and alter authentic birth certificates to develop and print 74 fraudulent birth certificates that sold for as much as $6,000 each.[1]

- In Florida, several children statewide were erroneously removed from the Department of Children and Families' missing list. Officials have not yet determined how many children were affected.[2]

- In New York, a help desk operator allegedly accessed more than 30,000 accounts and sold confidential banking and credit card data for purposes of identity theft.

[1] Claire Osborn, "State Statistics Clerk is Accused of Creating Phony Birth Records," *Austin American-Statesman,* 9 August 2002.

[2] Kathleen Chapman, "Teen Added to Missing List," *Palm Beach Post,* 23 October 2002.

> The Federal Bureau of Investigation (FBI) identified more than $2.7 million in fraudulent charges connected with this case.[3]

The increasing dependence placed on automated information increases the associated risks and costs if this information is compromised. Data security is becoming one of the highest risks an organization faces. Properly securing data requires management's recognition of the importance of information technology security and a commitment to properly securing the data in the most cost-effective way possible.

Chapter 1

Agencies Cannot Ensure the Security of Their Networks

Some health and human services agencies lack sufficient controls to ensure the security of their internal networks. As a result, there is a high risk that a user of the Health and Human Services Consolidated Network (HHSCN)—whether authorized or unauthorized—could use the HHSCN to access these agencies' internal networks and read, copy, modify, or delete confidential data.

What Is the HHSCN?

There are 16 state agencies and 225 private, public, and nonprofit organizations such as hospitals, health care providers, and corporations that are connected to this network. Other states that border Texas also have access to the HHSCN to view health-services eligibility information and services received by applicants in their states. There are approximately 55,000 workstations on the HHSCN.

Information resource managers from the participating agencies oversee the network through the HHSCN Governing Board.

The HHSCN operates as an Internet service provider; consequently, the agencies on the HHSCN are responsible for their own security. The highest vulnerability at any of the agencies on the HHSCN makes all the agencies vulnerable. These agencies need to strengthen their intrusion detection processes so they can quickly identify and resolve unauthorized access attempts.

The highest vulnerabilities we found were from inside the HHSCN. This is a result of the way some of the agencies' internal networks are structured. There were no high external vulnerabilities. This means that while any network has the potential to be exploited, the highest risk we found was from within the HHSCN. The greatest threat to any network is from internal users. Insiders are best qualified to compromise an agency's information. They have the means and skills to access the information, as well as the inside knowledge of an agency's systems and configurations.

- As referenced in *Information Security Magazine*, the Computer Security Institute stated that the average insider attack cost the target enterprise $2.7 million, compared with $57,000 for the average outside attack.[4]
- A study by the FBI and the Computer Security Institute on Cybercrime found that insiders are a major source of computer security breaches. This survey

[3] Keith Regan, "Insiders Pose Greatest ID Theft Risk," *Security Wire Digest,* 5 December 2002, Vol 4, No 90.

[4] Post, Jerrold; Shaw, Eri, and Ruby, Keven, "Managing the Threat From Within," *Information Security Magazine,* July 2000.

indicated that 71 percent of respondents detected unauthorized access to systems by insiders.[5]

Chapter 1-A

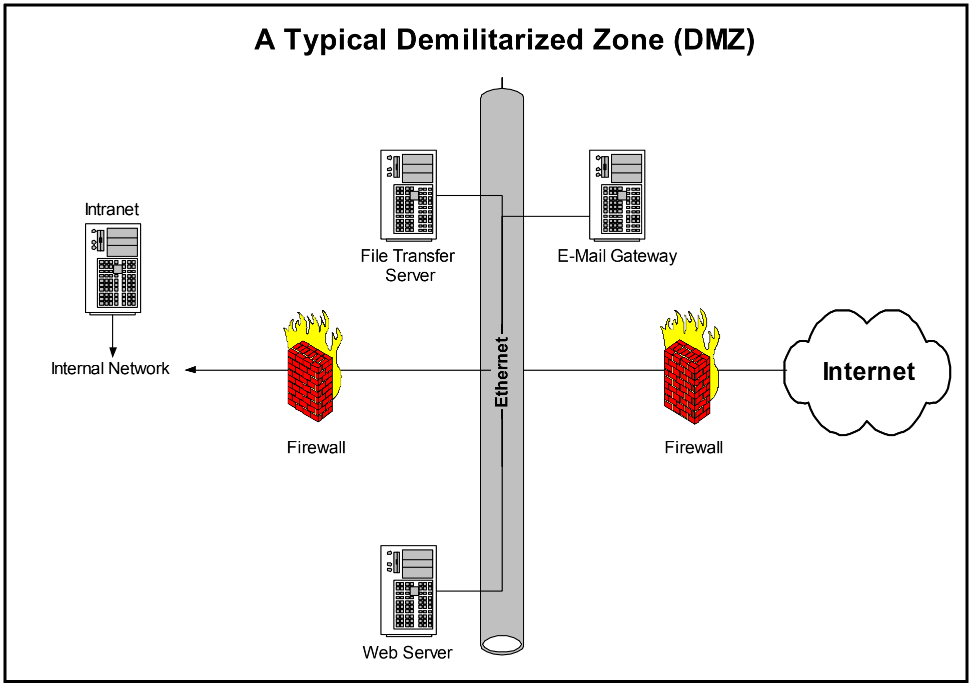
Network Configurations Do Not Provide Adequate Protection

Some agencies we audited lack basic network perimeter hardware or do not have their existing hardware configured to prevent unauthorized access. Perimeter security hardware primarily consists of firewalls, routers, and demilitarized zones (DMZ).

In some cases, firewall appliances were not in place. In other cases, agencies did not have their firewalls or routers configured to block unauthorized access by agencies on the HHSCN. An agency's first line of defense against threats to its network should be a firewall. A firewall provides more security than a router because it stops the transfer of and can make decisions about each packet of information that is being sent to the agency's network. A router, however, stops only packets that meet specific criteria.

In addition, some agencies do not have a DMZ to segregate their internal network from the Internet (see Figure 1). An agency that is connected to the Internet and hosts a Web site should have a separate server for its Internet services. This type of network architecture builds additional barriers, making it more difficult for unauthorized users to enter the agency's internal network. The lack of a DMZ makes it possible for Internet users to directly access Web and e-mail servers that are part of the agency's internal network, making the agency a target for hackers.

Figure 1



The Texas Administrative Code for Information Security (TAC 202) requires agencies to implement perimeter security controls that include measures such as a firewall, router, and DMZ.

[5] FBI Press Room, Congressional Statement on Cybercrime, 28 March 2000.

Recommendations

All health and human services agencies should evaluate their perimeter security controls and take the following actions if needed:

- Implement firewall appliances that will provide effective network perimeter security.
- Configure existing firewalls and routers to effectively block all other HHSCN users and traffic to prevent others from detecting their existence on the network.
- Develop a DMZ to protect their internal networks.

Chapter 1-B

Intrusion Attempts Are Not Formally Reviewed and Analyzed

The agencies we audited have intrusion detection systems and record attempted intrusions into their systems and applications. However, they do not have processes for reviewing and analyzing the intrusion information. As a result, they increase the risk that unauthorized activity will not be detected, analyzed, and properly resolved.

Effective intrusion detection both discovers and reports unauthorized activity, such as log-on attempts by someone who is not a legitimate user. Intrusion detection should detect misuse from internal users as well as intrusions from outside sources. Failure to detect penetration attempts quickly may give hackers the time they need to successfully penetrate an agency's systems.

TAC, Title 1, Section 202.7(f), requires the prompt investigation and documentation of security incidents and the reporting of these incidents to the Department of Information Resources (DIR) within 24 hours if there is a likelihood that the incidents could affect systems beyond the agency's control.

Recommendation

Agencies should develop processes for reviewing and analyzing the information collected by their intrusion detection systems. These processes should address the identification and analysis of security trends and ensure prompt reporting of security incidents to DIR as required.

Chapter 1-C

Wireless and Dial-In Access Increases Security Risks

The agencies we audited do not adequately secure wireless and dial-in (modem) access to their networks. While these access methods increase agencies' options for connecting authorized users, they also increase the risk of unauthorized use.

Our testing identified wireless access points that were broadcasting network names and transmitting unencrypted confidential data, making them a target for hackers. Wireless networks operate by transmitting a radio signal that can be captured by anyone within a certain distance who has the proper equipment. Securing wireless networks requires concealing network names and encrypting data. Some health and human service agencies have multiple locations that are across the street from or next door to one another. For them, properly secured wireless technology can be a low-cost way to increase connectivity.

Some agencies are not monitoring their networks for access by unauthorized modems. Dial-in capabilities allow anyone with a modem, valid access phone number, user ID, and password to log into the network. Hackers can gain access by using easily obtained or guessed user IDs and passwords. To mitigate the risks that come with using dial-in capabilities, agencies can scan their systems to detect unauthorized modems.

Recommendations

Agencies should:

- Secure and encrypt all wireless access points.
- Develop and enforce a wireless network policy.
- Implement strict standards and processes for dial-up access and conduct quarterly tests to detect unauthorized modems attached to the network.

Chapter 2

Agencies Lack Cost-Effective Security Management Programs

The agencies we audited do not ensure that they have cost-effective security management programs. During our audit, we found that, as a result, they do not always spend money for data security appropriately. They have not classified data (labeled agency data and grouped it into categories such as confidential, sensitive, public, and protected), assigned someone to be the data's "owner" (responsible for the data), or performed a cost-benefit analysis. These steps, as well as determining the resources necessary to secure the data, are the first steps toward developing a cost-effective information security program. Without cost-effective security, agencies are at risk of not spending funds appropriately for data security.

The primary objectives of an information security program are to preserve the availability, confidentiality, and integrity of data. If these objectives are ignored, an agency can be exposed to losses (such as fines and lawsuits). Confidential information could be disclosed and data integrity could be compromised either accidentally or intentionally. If information is not secured in a cost-effective manner, agency resources (people, assets, and funding) are negatively affected.

Security management is a responsibility shared by all employees. In violation of TAC, Title 1, Section 202.8 (d)(e), some agencies do not provide adequate security awareness training to help ensure that employees understand their responsibilities and the importance of security. Ongoing security awareness training is crucial to implementing the policies and procedures of an effective security management program.

Recommendations

Agencies, with executive management's knowledge and approval, should:

- Formally classify data, assign data ownership, and perform a cost-benefit analysis to determine the appropriateness of controls and the amount of resources needed to protect data and applications.

- Develop and implement a formalized security awareness training program. The program, which should be approved by the agency's security officer, needs to include documented training curriculum and training rosters to ensure that all users receive the training.

Chapter 3

Poor Access Controls Put Confidential Client Information at Risk

The agencies we audited do not adequately control users' and contractors' access to agency systems and data. Controls are not in place to ensure that the agencies consistently add, modify, or remove a user's access when they are hired, when they resign or are terminated, or when their job responsibilities change. In addition, some agencies failed to perform criminal background checks on employees and contractors before allowing them access to confidential client information.

The process of identifying users and allowing them to access only the systems or functions relative to their jobs is the basic premise of access security. This process also establishes user accountability. The risk associated with inadequate access controls is that the integrity, confidentiality, and availability of data and resources may be compromised.

Insufficient access controls threaten data integrity by allowing individuals access to applications or functions outside of their normal job responsibilities. Allowing an individual to view or download sensitive data may compromise confidentiality. By not controlling access, an unauthorized individual can compromise availability by altering administrative settings or making changes to the operating system, databases, or telecommunications software.

Recommendations

Agencies should develop and implement written procedures for:

- Providing users access, including creating new user accounts, modifying security profiles, and deleting accounts.

- Monitoring inactive accounts.

- Periodically reviewing and confirming users' access rights within all systems and applications.

- Conducting criminal background checks on employees and contractors if required.

Chapter 4

Disaster Recovery Plans Are Adequate to Ensure Recovery

The agencies we audited have documented disaster recovery plans that define roles, responsibilities, and risks associated with an interruption to selected critical systems.

The disaster recovery plans and business resumption plans at these agencies have the required disaster recovery procedures in place to ensure that emergencies and natural disasters will not cause significant disruptions to their critical systems or operations. These plans are tested regularly.

We visited the West Texas Disaster Recovery and Operations Center (WTDROC) to evaluate its disaster recovery processes for its clients, which include other state agencies. Several state agencies also house their mainframes at WTDROC. We determined that WTDROC has developed and tested disaster recovery plans for its client agencies to ensure that emergencies and natural disasters will not cause significant disruptions to the State's critical systems.

Chapter 5

Audited Agencies Have Good Physical Security Over Their Computer Equipment

The audited agencies' facilities provide suitable physical surroundings to protect information technology (IT) equipment and people against man-made and natural hazards. We noted only minor issues in the physical security walk-throughs and TAC compliance reviews we performed. We discussed these minor issues with the IT departments' management, and many were already addressed before we concluded our fieldwork.

We also reviewed physical security at WTDROC and found that its physical security is adequate to protect its equipment and people. Our conclusion of adequate physical security applies to all agencies with information and/or hardware located at WTDROC.

Other Information

Objectives, Scope, and Methodology

Objectives

The objectives of the audit were to determine whether the selected agencies:

- Have adequate access and security controls for the selected major systems to ensure that critical information is sufficiently protected from loss or misuse.
- Have developed and tested disaster recovery plans to ensure that emergencies and natural disasters will not cause significant disruptions to agency systems.

Scope

The scope of this audit included the major client information systems at selected health and human services agencies. We also evaluated physical security and disaster recovery at the West Texas Disaster Recovery and Operations Center and network security over the Health and Human Services Consolidated Network as it related to these agencies.

Methodology

Our methodology consisted of interviewing staff at the various agencies, field offices, and regional offices; reviewing disaster recovery and information security plans; reviewing policies and procedures, network maps, and other agency documents; inspecting data centers; and conducting internal and external network scans and wireless leakage tests to identify potential system vulnerabilities.

Project Information

We conducted fieldwork from July through October 2002. We performed this audit in accordance with generally accepted government auditing standards.

Distribution Information

Legislative Audit Committee

The Honorable Tom Craddick, Speaker of the House, Chair
The Honorable David Dewhurst, Lieutenant Governor, Vice Chair
The Honorable Teel Bivins, Senate Finance Committee
The Honorable Bill Ratliff, Senate State Affairs Committee
The Honorable Talmadge Heflin, House Appropriations Committee
The Honorable Ron Wilson, House Ways and Means Committee

Office of the Governor

The Honorable Rick Perry, Governor

This document is not copyrighted. Readers may make additional copies of this report as needed. In addition, most State Auditor's Office reports may be downloaded from our Web site: www.sao.state.tx.us.

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

The State Auditor's Office is an equal opportunity employer and does not discriminate on the basis of race, color, religion, sex, national origin, age, or disability in employment or in the provision of services, programs, or activities.

To report waste, fraud, or abuse in state government call the SAO Hotline: 1-800-TX-AUDIT.