STATE OF ARIZONA
OFFICE OF THE
AUDITOR
GENERAL

# Department of Economic Security
Information Security

REPORT
HIGHLIGHTS
PERFORMANCE AUDIT

## Subject

Information security includes controls over employees' and other users' access to data, protection against virus attacks and hackers, procedures for making changes to computer programs, and disaster recovery plans.

## Our Conclusion

To ensure that the information contained in the Department's IT systems is adequately protected against employees' misuse, hacker intrusions, viruses, or other damage, the Department needs to take precautions such as ensuring all central security staff know their duties and are trained to perform them, installing virus protection on all computers, improving documentation of programming changes, and completing its disaster recovery plan.

2005

July • Report No. 05 – 04

# Controls Over Data Security Need Improvement

The Department estimates that it serves over 1 million children, adults, and families each month, relying on more than 80 different computer systems to perform numerous functions involving sensitive client data. These functions include tracking child welfare cases, determining eligibility for Temporary Assistance for Needy Families(TANF), and monitoring bill payments for individuals with developmental disabilities. In addition, the Department processed over $48 million in cash assistance and unemployment payments per month in fiscal year 2004.

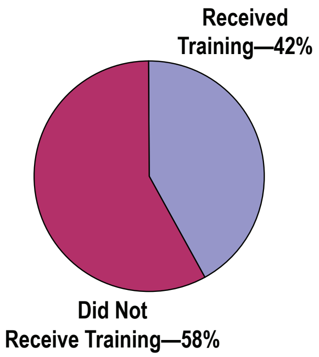
**Access controls**—Access controls help ensure that only authorized persons have access to the systems and that they can access only the data needed to do their jobs. For example, they should ensure that security privileges, including the ability to create, update, or delete user accounts and reset passwords, are limited only to people who need this function to perform their job duties.

**Controls should be strengthened**—Control weaknesses were found throughout the Department and indicate that it is not in compliance with Arizona's Government Information Technology Agency (GITA) state-wide security standards. Weaknesses include:

- Keeping old or unused user accounts—More than 1,300 accounts have not been used in over a year. More than 1,100 accounts have never been used.
- Not updating passwords—Although passwords should be changed every 30 days, more than 200 accounts are not required to change passwords, and one employee has not changed his password in over 2 years.
- Giving too many people special security administrator privileges—Over 80 people can create or change user accounts for other employees.

**Need for greater central oversight**—Historically, the Department has not provided central oversight of security functions. However, in September 2003, it established an Information Security Administration that recently has begun to perform some compliance reviews and assessments of information security throughout the Department. This group should develop a schedule of regular reviews and a follow-up process to ensure that its recommendations are implemented. In addition, the Department should consider establishing an internal IT audit function to help it ensure that it has effective and efficient security controls, and should also consider hiring an outside contractor to conduct a security assessment.

Employees Receiving Security Training



Further, while the Department has appointed security representatives throughout the agency, it only recently developed a draft job description to define what the positions should do and what expertise is required. One of the divisions employs security representatives with IT backgrounds, while other security representatives are support and clerical staff.

**Need for training and background checks**—GITA standards and department policy require computer security training before any employee has computer access. However, according to a random sample of training records, only 42 percent of employees had taken the training.

Further, while criminal background checks are a valuable tool in assessing an employee's trustworthiness, the Department does not have legal authority to order such checks for its security representatives.

## Recommendations

The Department should:

- Develop a schedule of regular compliance reviews and assessments and a follow-up process to ensure its recommendations are implemented.
- Establish an internal IT audit function.
- Consider having an outside contractor conduct a security assessment.
- Ensure that security representatives know their duties and how to perform them.
- Ensure that all new employees receive mandatory computer training.
- Seek statutory or executive order authority to conduct background checks on IT personnel.

# LAN and Computer Information Not Adequately Protected

Of 57 computers tested for updates:

- 55 were missing 1 or more critical updates.
- 7 were missing more than 20 updates.
- Some were missing updates since 2003.

A local area network (LAN) connects computers within a limited geographic area, such as within an office or a city. Separate LANs can be connected to form larger LANs, as is the case at the Department, where there is a state-wide network that brings together the Department's many offices.

The greatest threats to computers and networks are viruses, hackers, and software downloaded from the Internet.

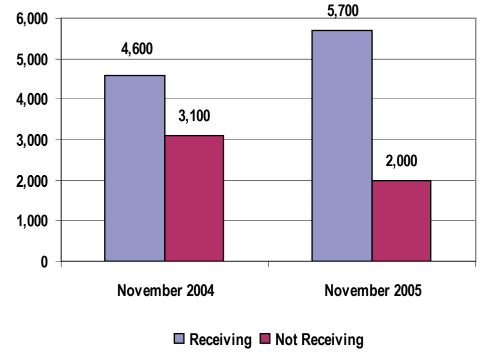
**Security patches not installed**—The Department needs to better protect its computers and LANs. The first step is installing security patch updates on all computers. Security patch updates correct vulnerabilities in computer operating systems and are issued regularly by software companies as vulnerabilities are identified. For example, a February 2005 update corrects a weakness that may allow a hacker to remotely take control of a computer.

In April 2005, the Department identified an automated computer tool to permit it to centrally control and install security updates. It plans to implement the tool in January 2006.

**Virus protection is improving**—Virus protection software can also be centrally controlled. Since 2002, the Department has purchased an annual license for an entity-wide version of virus protection to install on every computer. The Department is in the process of moving all of its computers to this centrally controlled process and has increased the number of computers receiving daily virus updates. However, 2,000 computers are still not receiving the updates from the centrally controlled software.

**Controls needed over Internet downloads**—An employee who downloads free software from the Internet potentially exposes the computer to adware, spyware, or other harmful software. These types of programs can permit outside users to discover passwords, slow down or lock up a system, or install harmful software. Six of 20 computers auditors reviewed had nonbusiness-related software that had been downloaded from the Internet. While the Department has an acceptable use policy that prohibits staff from downloading software unless approved by local IT management, it needs to ensure that its employees understand the policy and monitor compliance with it.

Computers Receiving Daily Virus Updates



## Recommendations

The Department should:

- Ensure that all computers have up-to-date security patches installed and periodically monitor updates.
- Install entity-wide virus protection on all computers.
- Ensure employees understand the Department's acceptable use policy and monitor compliance with it.

# Department Could Improve Management of Computer Program Changes

The Department frequently needs to change its computer programs in response to changes in state and federal requirements, or to correct errors and inefficiencies. The Department made 991 programming changes in the first 6 months of fiscal year 2005. Inadequate management of such computer program changes can lead to programming errors and inefficiencies.

The current process for making programming changes varies greatly among the Department's 20 project teams. The lack of a uniform, standardized process for changes increases the risk of having inadequate controls over some program changes.

A critical component of program changes is adequate testing by the programmer and the end user so that the change works the way it is supposed to. However, department programmers typically conduct only limited testing.

The Department is addressing program change oversight by developing a written program development methodology and management policy. It also acquired an automated testing tool in June 2005.

### Recommendations

The Department should:

- Standardize its program change process.
- Implement its automated program change testing tool.

## Disaster Recovery Has Improved

Disaster recovery planning allows critical services to continue in the event of damage to an agency's computer systems. Damage to or loss of the Department's computer systems would disrupt services to over 1 million people and affect over $48 million in TANF and unemployment payments each month as well as child support and food stamp payments.

A comprehensive disaster recovery plan should include:

- Identification of critical transactions and procedures for processing them.
- Designation of an alternative computer facility or "hot site."
- Development of plans to test the disaster recovery's effectiveness.
- Scheduling frequent backups of system information and storage of backups at remote sites.

The Department's progress in disaster recovery planning has been slow because of employee turnover. However, in 2004 the Department hired a disaster recovery manager, obtained funding, contracted for backup data storage and emergency hot sites, and established a timetable for completing the planning.

The Department began daily backups of critical systems in June 2005, and also conducted a test at its emergency hot site to test its mainframe and network recovery procedures.

However, current planning activities do not provide comprehensive solutions. The Department estimates that it could take a minimum of 2 weeks to restore mainframe and network services at the temporary hot site, and the contractor guarantees to make the hot site available for only 6 weeks.

### Recommendations

The Department should:

- Update and complete its disaster recovery planning software.
- Ensure its testing plan is included in planning software.

TO OBTAIN
MORE INFORMATION

A copy of the full report
can be obtained by calling
**(602) 553-0333**

☎

or by visiting
our Web site at:
www.auditorgen.state.az.us

Contact person for
this report:
Shan Hays