STATE OF ARIZONA
OFFICE OF THE
AUDITOR
GENERAL
INTEGRITY • ACCOUNTABILITY • MAKING A DIFFERENCE

Arizona Department of Revenue—Security of Taxpayer Information

REPORT HIGHLIGHTS
PERFORMANCE AUDIT

Our Conclusion

To perform its business functions, the Arizona Department of Revenue (Department) handles large volumes of both paper and electronic sensitive taxpayer information. The volume and nature of this sensitive information make the Department a potential target for attack by malicious individuals or organizations looking to access and/or steal this information. The Department has taken steps to protect taxpayer information; however, we identified vulnerabilities that leave taxpayer information at risk. In order to address these vulnerabilities, the Department should improve its information technology (IT) security, continue to develop its information security program, and enhance the physical security of taxpayer information.

2015

September • Report No. 15-116

Department needs to improve its IT security

Sensitive information and systems exposed because of IT security weaknesses—Security weaknesses can be exploited to gain access to and/or compromise IT systems, which can result in considerable costs to both organizations and individuals whose information is accessed. By simulating common attack patterns, we were able to gain unauthorized access to sensitive taxpayer information by exploiting weaknesses in the Department's internal IT systems. Through this effort, we found that we could take over user accounts that could be used to view, alter, or delete sensitive taxpayer information. We also performed successful social engineering techniques against department employees, which revealed weaknesses in some of the Department's controls and IT security training.

Improvements needed to Department's IT security processes—Although the Department has established various processes to help secure its IT systems, it needs to improve its IT security practices in several areas:

- **Documented processes needed for securely maintaining IT systems**—The Department has some processes for reviewing IT system vulnerabilities; applying patches, or updates and fixes, to systems; and configuring IT systems. However, the Department needs to document and/or enhance its policies and procedures in these areas.
- **Inadequate process for restricting access to only authorized users**—Although the Department performs some aspects of access control, we identified multiple deficiencies that provide department staff excessive access to information on the Department's IT systems, including some sensitive files not restricted on the Department's network, active user accounts that were unused or linked to terminated employees, and passwords that were older than allowed by department policy.
- **Insufficient IT system log monitoring**—Monitoring logs of critical IT system activities helps organizations track events on IT systems and networks and detect improper actions by any IT system user, whether staff or nonstaff. However, the Department performs only limited log monitoring.

Recommendations

The Department should:

- Develop and implement written policies and procedures to improve its vulnerability assessment processes, patch management, and configuration control;
- Improve management of access controls across IT systems; and
- Develop and implement a continuous log-monitoring program for critical IT activities.

Department should continue developing its information security program

Information security officer (ISO) position's authority strengthened—In January 2015, the Department enhanced the authority of its ISO position, which is responsible for overseeing department information security efforts. Although the ISO's responsibilities are consistent with IT standards and best practices, the ISO has historically not overseen IT security for some IT systems managed by certain divisions. The Department should ensure the ISO regularly monitors department-wide compliance with information security program policies and procedures.

Department has begun developing information security program—Consistent with state requirements, the Department has begun developing an information security program by drafting additional information security policies. As of July 2015, the Department had drafted all of its policies but had not yet finalized some of them and had not yet developed most of the related procedures. For example, the Department lacked adequate procedures in four key security program areas we reviewed: data classification, risk assessment, information security awareness education and training, and incident response. IT standards and best practices recommend developing an action plan to guide the development and implementation of an information security program, which includes identifying tasks that need to be accomplished, the resources required to accomplish these tasks, and scheduled completion dates for the milestones established. Therefore, the Department should develop and implement an action plan and milestones to finish developing its information security program.

Recommendations

The Department should:

- Ensure the ISO position regularly monitors department-wide compliance with information security program policies and procedures; and
- Implement an action plan to complete the development of its information security program.

Department has taken steps to ensure physical security of taxpayer information, but some improvements needed

Department has taken steps to ensure physical security of taxpayer information—Because the Department keeps both paper and electronic taxpayer information in each of its four buildings, it is important that areas containing this information be secure. The Department uses several security measures, such as security guards and cameras, physical barriers, and badge access readers, to limit physical access to its buildings and taxpayer information. The Department also moved its tax-processing division out of its main building to an unmarked location that provides for enhanced security.

Additional measures needed to safeguard taxpayer information—We identified some areas where the Department's physical security can be strengthened. For example, although the Department requires badge access for employees to access most areas of its buildings, the Department did not document the destruction of employee badges when employees left the Department's employment. Additionally, not all badges were deactivated in a timely manner. We also found that, although the Department has a clean-desk policy requiring employees to secure any documents containing taxpayer information when they leave their workspace and a procedure regarding clearing off fax machines, employees did not always comply with this policy and procedure, sometimes leaving taxpayer information in plain sight. Additionally, there is no procedure for clearing sensitive information off copy machines/printers.

Recommendations

The Department should:

- Document its destruction of former employees' badges and ensure they are deactivated in a timely manner;
- Ensure employees comply with its clean-desk policy and fax machine procedure; and
- Expand the fax machine procedure to include copy machines/printers.