ARIZONA Auditor General
Making a Positive Difference

REPORT HIGHLIGHTS
Performance Audit
April 2017

Arizona Department of Economic Security
Information Technology Security

CONCLUSION: The Arizona Department of Economic Security (Department) has a significant responsibility to safeguard its information technology (IT) systems and the data contained in them from misuse or attack because of the volume and nature of the sensitive data it maintains. Although the Department has established various IT security processes to help protect its IT systems and data, by performing common attack patterns, we identified weaknesses that allowed us access to these IT systems and sensitive data, including social security numbers and confidential health information. Additionally, the Department lacks an information security program as required by state policy. Establishing such a program would help ensure the Department sufficiently protects its IT systems and data. Finally, our in-depth review of three key policy areas—data classification, incident response, and security awareness education and training—found that the Department had not developed or fully developed associated procedures and had not incorporated some best practices within its incident response policy.

Department responsible for safeguarding its systems and data

As of December 2016, the Department reported using more than 120 IT systems or applications to store and process large volumes of sensitive data to administer various programs. These programs provide many services, such as unemployment insurance benefits, cash and/or nutrition assistance, child care assistance, and adult protective services, to assist more than 2 million Arizonans in need annually. Because of the volume and nature of the sensitive data the Department maintains—which includes names, social security numbers, driver license or state identification numbers, mailing addresses, and other information—it is a potential target for malicious attacks. The Department's responsibility to protect its data is specified in various federal and state laws and regulations, which include requirements for safeguarding health information and federal tax information.

Department should improve security processes and controls over its IT systems and data

Department's IT systems and sensitive data exposed because of security weaknesses—By simulating common attack patterns and exploiting security weaknesses, we accessed the Department's core IT systems and the sensitive data contained in them. Specifically, we exploited a weakness in the Department's network and gained unauthorized access to IT systems and sensitive data. With this access, we could control all network user accounts and view, alter, or delete confidential health information and other sensitive data. We also gained unauthorized access to sensitive data by exploiting security flaws in one of the Department's external web-based applications. Finally, we gained unauthorized access to IT systems and sensitive data through various social engineering techniques that requested department employees to perform actions and/or provide information needed to gain access.

Department has various IT security processes but should take steps to strengthen them—Although the Department has established various IT security processes and took steps to fix the specific security weaknesses we identified, its processes are not sufficiently robust to effectively identify, prevent, and remediate IT security weaknesses. Therefore, the Department needs to take several steps to more effectively secure its IT systems and the sensitive data contained in those systems. Specifically, the Department should improve three key security management processes: (1) vulnerability management, which involves systematically identifying, reviewing, and correcting IT system vulnerabilities; (2) patch management, which entails applying patches, or updates and fixes, to systems to ensure they remain secure; and (3) system configuration, which helps to ensure that the settings that control how systems operate are securely configured. In addition, the Department should strengthen its process for restricting access to its IT systems, including ensuring that user accounts for terminated employees are disabled or removed as soon after the employee leaves as is practical. Further, the Department should develop and implement a continuous process for monitoring system activity and policies, procedures, and practices for securely developing web-based applications.

Recommendations

The Department should develop or continue to develop and implement written policies and procedures for:

- Improving its vulnerability assessment, patch management, and system configuration processes;
- Ensuring the access-removal process is properly conducted;
- Establishing a continuous monitoring program for critical IT activities; and
- Developing, securing, and testing web-based applications.

Department should establish an information security program

Department has not established an information security program—To help ensure IT security state-wide, the Arizona Department of Administration, Arizona Strategic Enterprise Technology Office (ASET) requires state agencies to develop and implement an information security program. An information security program would help ensure that the Department has processes for identifying and safeguarding its IT systems and data against security vulnerabilities. Although the Department had developed a general policy outlining some requirements for an information security program, it lacked an overall security program that was consistent with ASET's requirements and best practices. For example, the Department had not conducted a department-wide IT risk assessment or developed procedures for doing so on a regular basis, and it had not adequately established the authority and responsibilities for information security.

Department should create written plan for developing an information security program—To help ensure the Department's IT systems and data are sufficiently protected, the Department should establish a written plan for developing and implementing a department-wide information security program. Consistent with ASET requirements, this plan should also address areas such as risk assessment; staff authority, roles, and responsibilities related to IT security; and the resources needed to implement an information security program.

Recommendations

The Department should:

- Establish a written plan for developing and implementing a department-wide information security program;
- Develop and implement department-wide IT risk assessment procedures;
- Further define information security program authority, roles, and responsibilities; and
- Ensure that needed resources are available to implement the program, such as staffing and budget.

Department should enhance efforts to establish information security policies and procedures

Department has not adequately implemented policies and procedures in three key information security areas—Although the Department has drafted or finalized policies for the 17 information security areas required by ASET, our review of three key areas—data classification, incident response, and information security awareness education and training—found that the Department had not incorporated some best practices within its incident response policy, and had not developed or improved the associated procedures to fully implement these policies.

Department had not implemented policies and procedures in other information security program areas—Our high-level review of several other ASET-required areas needed for a strong information security program found similar issues with inadequate, undeveloped, and/or unimplemented policies and procedures. For example, the Department's contingency planning policy, which states how it would restore unexpectedly unavailable data and operations, only applies to some systems and is missing critical best practices elements, such as detailed recovery procedures for restoring data. Further, the Department's written procedures for applying patches—or updates and fixes—to its IT systems inadequately address updating software and employee workstations. Without adequately developing policies and procedures to secure its IT systems and data, the Department is at a higher risk of a data breach.

Recommendations

The Department should:

- Further develop and implement information security policies and procedures for the areas of data classification, incident response, and information security awareness education and training; and
- Ensure its written plan for developing and implementing a department-wide information security program includes a process for adequately developing and implementing all ASET-required policies and procedures.