Scott Fitzpatrick
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of Statewide Security Training Awareness

Background

According to the Office of Administration Information Technology Services Division (ITSD), security awareness training is the basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. Security awareness training teaches employees how to protect information technology systems and agency data, and develops skills and knowledge, enabling employees to perform their jobs more securely. Security awareness training also improves the security posture of the enterprise [the state], and facilitates the implementation of appropriate security policies and procedures.

The ITSD was formed in January 2005 to consolidate information technology (IT) staff and funding. This consolidation primarily covered most executive branch agencies. The ITSD provides services, including security awareness training services, to its consolidated entities (CEs). Non-consolidated entities (NCEs), which are structurally independent of the ITSD, maintain their own internal IT departments that provide services, including security awareness training services, to their employees. Despite their structural independence, many NCEs remain in communication with, and sometimes enter into selective coordination with, the ITSD. The overall structure and distinct roles between the ITSD, CEs, and NCEs present general challenges to achieving statewide security awareness.

Scope and Methodology

The scope of our audit included, but was not limited to, the year ended June 30, 2023.

To evaluate the state's policies and procedures related to security awareness training, we reviewed written ITSD policies and procedures available, and interviewed the management of each NCE to understand their security awareness training activities. We also interviewed ITSD management on behalf of the CEs. We obtained all 18 CEs' training records for the 6 months ending June 30, 2023. To analyze results, we compared the training records to personnel records from the state's SAM II Human Resources system to determine the number of monthly security trainings each employee had completed during the 6-month test period. We limited our analysis to approximately 30,000 individuals who were actively employed, and remained with their CE, for the full 6 months. We performed procedures to ensure the data was complete to support our audit objectives, but reviewing internal controls of these systems was not part of our objectives.

To evaluate the ITSD's monitoring controls over security awareness training we interviewed ITSD management on behalf of the CEs, and identified and evaluated related policies and procedures.

Consolidated Entity Training Not Being Consistently Completed, Oversight Improvements Are Needed

CE employees did not consistently complete monthly security awareness training required by ITSD policy. A review of training results for the 6 months ending June 30, 2023, found approximately 20 percent of employees did not complete any of the 6 monthly trainings during that period, and 30 percent of employees received less than half of the required trainings in the test period.

Additionally, the ITSD does not provide oversight of the CEs' administration of cyber security awareness training. On May 1, 2023, the ITSD issued an updated security training policy with an additional clarification that "audits and assessments will be performed" by "authorized organizations" to help ensure compliance with the policy. However, this policy was rescinded by ITSD in June 2023 and has not been reissued, but is currently being reevaluated and is in draft form.

Based on our review of CE training records, most CEs have employees who were unofficially exempted, and thus, lacked the expected opportunities to receive and complete monthly security awareness training.

Non-Consolidated Entity Training and Phishing Testing Weaknesses

Four of 16 NCEs do not provide or obtain ongoing security awareness training for their employees. In addition, 9 of 16 NCEs do not perform or obtain phishing testing on their employees. Most of the remaining 7 NCEs contracted with vendors to perform phishing testing on their employees. The 4 NCEs that do not provide security awareness training to their employees are also included in the 9 entities that do not do phishing testing. As a result of these weaknesses, state resources such as data, systems, and/or monetary funds are at increased risk of loss or exposure.

Because of the nature of this audit, no rating is provided.

Scott Fitzpatrick
Missouri State Auditor

RECOMMENDATION SUMMARY

Recommendations in the audit of Statewide Security Awareness Training

Consolidated Entity Training Not Being Consistently Completed, Oversight Improvements Are Needed	The Office of Administration Information Technology Services Division (ITSD) update its security awareness training policy to require oversight procedures for consolidated entity (CE) security awareness training to ensure required trainings are being completed, and clarify whether CEs are allowed to exempt certain employees from training requirements.
Non-Consolidated Entity Training and Phishing Testing Weaknesses	Non-consolidated entities (NCEs) not performing security awareness training and phishing testing should consider the ITSD's security awareness training policy and phishing testing efforts and establish policies and procedures to ensure training and testing are completed regularly for their employees. NCEs not currently providing security training or phishing testing should consider using ITSD as a resource to implement such procedures.