Insider Threat Risk Management (ITRM):

Arizona Department of Administration

Arizona Strategic Enterprise Technology

July 18, 2018

ADOA-ASET

Arizona Strategic Enterprise Technology

The ADOA ASET Enterprise Security team under the leadership of the Statewide CISO, Mike Lettman, continues to transform and innovate the way the State manages and protects itself from cyber security risks.

The approach used is the consistent application of industry best practices to:

- Identify gaps and information via agency Information Security Officers (ISO's)
- Strategically source enterprise tools and services that enhance the speed, reduce costs, and increase the effectiveness of cyber security procurements and implementations

Background

Last year, collaborating with State agencies, the team successfully deployed 14 security controls that provided agencies with cost effective, best in class, enterprise solutions. While these solutions have demonstrated a clear value to improve the State's risk posture, some gaps still remain.

This year, to address the identified gaps, the team is requesting approval to leverage $ 3.1m of the $ 6.9 m allocated budget (approved by the legislators) to deploy 3 enterprise insider threat controls to fill the existing gaps where the State of Arizona is at risk:

- User Behavior and Entity Analytics UEBA)
- Cloud Access Security Brokers (CASB)
- Phishing Simulations

User and Entity Behavior Analytics (UEBA)

UEBA solution collects and analyzes the behavior of users, groups and devices to establish baselines and identify unusual behaviors.

By learning what is considered normal behavior, the solution makes it possible to detect and identify security risks and threats such as:

- Password theft
- Rogue employees/insider threats
- System administrator access abuse
- Malicious hackers
- Data breaches

Cloud Access Security Brokers (CASB)

CASB extends State of Arizona information security controls and policy compliance into cloud-hosted services closing a gap in controls that currently exists for cloud solutions.

Acting as intermediary between "us and the cloud" the solution alerts on and takes action to protect sensitive data. Key gains in controls include:

- Data Loss Protection (DLP) capability within authorized cloud services
- Automated actions taken in near-real time to protect sensitive data
- Protections applied anywhere a user is accessing authorized cloud services
- Activity tracking within authorized cloud services
- Identifies unauthorized cloud services being used by employees (Shadow-IT)
- Increased compliance with regulatory requirements

Phishing Simulation

Phishing simulation sends no-risk phishing emails to employees. Employees who are tricked into clicking on simulated links are required to complete security awareness training.

The phishing simulation solution benefits include:

- Assess - Simulations allow you to quickly and effectively assess how susceptible employees are to phishing and spear phishing attacks. End users who fall for simulated attacks are automatically presented with a Teachable Moment, which offers "just-in-time" guidance that lets users know what they did wrong and offers tips to help them avoid future threats.
- Educate **-** Security awareness training programs include targeted anti-phishing training as well as organization-wide education.
- Reinforce - Reinforcing best practices is critical to improving retention.

What's Been Accomplished:

Technology options and vendors researched

- Research and requirement gathering, vendor demonstrations, revised requirements, proof of concepts, quotes obtained
- 3 solutions identified
- JLBC Favorable review for the funds

What's Planned:

- Submit purchase requests, deploy tools enterprise-wide by June 2019

Benefits:

- Protect State data
- Strengthen the overall security position

Financials

Description	FY18	FY19	FY20*
CASB	$1,511,300	$0	$863,600
UEBA	$1,500,806	$0	TBD
Phishing	$96,096	$0	$48,048
TOTALS	$3,108,202	$0	$911,648

The three new controls will be purchased, bundling two years of licensing, using a portion of the available FY 2018 appropriation from the Automation Projects Fund. This approach has a $0 cost in FY 2019. This strategy allows ADOA-ASET to review the effectiveness of the solutions, and account for changes in technology or threat patterns prior to committing to additional costs.

*FY20 expenses will only be realized if continued appropriations are made. Contracts are written with funds availability clauses.

Questions?