ARIZONA
DEPARTMENT OF ADMINISTRATION
TECHNOLOGY

NASCIO 2021 State IT Recognition Awards
Cybersecurity

Enterprise Security Program Advisory Council (ESPAC)

Title: Enterprise Security Program Advisory Council (ESPAC)
Category: Cybersecurity
State: Arizona
Contact: Bryan Beach
Bryan.Beach@azdoa.gov
(602) 316-8369
Start date: 2/2019
End date: ONGOING

EXECUTIVE SUMMARY

Situation

Cybersecurity is an ongoing priority for the State of Arizona. As cyber threats evolve, individuals and organizations must adapt to the landscape. In order to ensure that sensitive data and systems are adequately protected, the State of Arizona takes a multi-tiered approach by using best-of-breed cybersecurity tools and providing knowledge and training to state employees, ensuring the presence of both a technical and human firewall that can block many cyber attacks from being successful. Additionally, collaboration within the state fosters agency participation in enterprise-level decision making, partnerships with SLTTs, information sharing, and statewide strategy implementation.

Security breaches can result in unauthorized access to sensitive information and systems, leading to significant financial damages or impacts to crucial government services. Within the State of Arizona, it is especially vital that the personal information of its citizens be protected at all times, and critical services remain available. To build this layer of protection and gain the trust and confidence of citizens, the use of sophisticated cybersecurity tools and the capabilities provided by well-trained employees are absolute necessities at all levels of government. Specific cybersecurity focuses in the State of Arizona include:

1. Improving efficiencies
2. Increasing Statewide accountability
3. Enhancing public safety
4. Fostering innovation
5. Leveraging partnerships

Problems

A lack of adequate cybersecurity information sharing is an issue that impacts even the most mature state agencies. Additionally, several agencies had expressed feelings of being excluded from enterprise-wide strategy decisions being made, which could significantly impact their operations. With support from the highest levels of government, the State of Arizona recognized the need to focus on working together to achieve mutual goals.

Solution

The Enterprise Security Program Advisory Council (ESPAC) at the State of Arizona actively collaborates with all levels of government to ensure that cybersecurity programs are developed and maintained effectively to keep pace with evolving threats. Moreover, Arizona Governor Doug Ducey created the Arizona Cybersecurity Team (ACT) that subsequently published a comprehensive list of recommendations to protect Arizona against cyber threats, which also included enhanced information sharing and collaboration efforts throughout the State.

CONCEPT

The Enterprise Security Program Advisory Council (ESPAC) was initiated by the Governor's Office for the benefit of all state agencies to unify the state's cybersecurity strategy. The purposes of the council include:

- Providing a mechanism for members to advise and inform the State CISO, the Governor's Office, Legislature and other interested state bodies on matters related to security information technology planning, policies, and standards.
- Providing a forum for the above described community to address issues of mutual interest and share information with one another.
- Fostering cross-agency and cross-jurisdictional collaboration and support with the goal of strengthening the IT security leadership community in their shared support of the business of the state.

ESPAC, with statewide leadership support from the Governor's Office and the State CISO, works to secure funding that provides security tools to state agencies. This partnership helps realize economies of scale, drives adoption and mature operationalization through peer support, and reduces vulnerabilities through collaboration and the adoption of standardized statewide policies.

In support of agency IT and cybersecurity staff, ESPAC and the Enterprise Security Team work with state agencies to share information and resources for maintaining cybersecurity throughout Arizona to protect systems and data. ESPAC sets the statewide standards and policies, and the Enterprise Security Team works alongside the agencies to implement statewide standards and enterprise security tool adoption. Subsequently, security gaps are addressed and remediated, thereby keeping citizen data safe.

Cybersecurity solutions, including enterprise security tools, are selected and configured to best protect the state's resources and data. Using a multi-tiered approach, software and other technologies are adopted and maintained for optimal protection. ESPAC and the Enterprise Security Team have successfully facilitated the implementation and ongoing support of 17 enterprise cybersecurity tools across more than 90 state agencies. The success of the program has resulted in cost savings to taxpayers, and increased system and data protection.

Most cyber attacks are successful when the end user invites an adversary in through the front door by unintentionally clicking on a link, or unknowingly downloading malicious content. Making cybersecurity awareness training and anti-phishing campaigns mandatory for every state employee, ESPAC has improved frontline defenses by effectively expanding the Arizona cyber

team to all 36,000 state employees. By providing these same tools and training to local and tribal governments in Arizona, another 30,000 individuals are standing ready and are prepared to protect state data. This level of defense is what the industry refers to as the human firewall. While no cybersecurity program is truly impregnable, the State of Arizona remains vigilant in its efforts to defend against cyber attacks and respond to emerging threats. As hackers continue to step up their game, ESPAC continues to adapt its tactics to protect citizen data from these threats.

In order to increase accountability across Arizona, ESPAC has assisted with the development and adoption of statewide policies governing IT security in alignment with NIST Special Publication 800-53 security and privacy controls. These policies include:

- Data Classification
- Information Security Program
- System Security Acquisition and Development
- Security Awareness Training and Education
- System Security Maintenance
- Contingency Planning
- Incident Response Planning
- Media Protection
- Physical Security Protections
- Personal Security Controls
- Acceptable Use
- Account Management
- Access Controls
- System Security Audit
- Identification and Authentication
- System and Communications Protections
- System Privacy

ESPAC also developed and approved implementation standards for each of the 17 enterprise cybersecurity tools provided to state agencies for more operational level guidance. These standards follow the SMART principle: Simple, Measurable, Actionable, Relevant, and Time-based. The standards provide further specifics on “how” the agencies should use the tools to ensure they are in compliance with the policies.

For more information, visit: https://espac.az.gov/

SIGNIFICANCE

Through a cyber grant award from the Arizona Department of Homeland Security (AZDOHS) and US Department of Homeland Security, local and tribal governments in Arizona who apply are able to obtain available cybersecurity resources to keep their systems and data safe from bad actors attempting to identify and exploit possible vulnerabilities.

For the previous two years, 50+ local and tribal governments have participated in the cyber grant program awarded to the Arizona Department of Administration (ADOA) in partnership with ESPAC to leverage the buying power and expertise of the Enterprise Security Team and the multi-jurisdictional volunteer liaison team. Many local and tribal governments have gaps in their cybersecurity programs because they do not have the resources, knowledge, or the budget to purchase and install sufficient cybersecurity tools that protect their data and their networks from compromise. Since local, tribal, and state government systems interconnect to each other, all are at significant risk of attack.

Cybersecurity tools available to Arizona local and tribal governments, at no cost to them, include:

- Anti-Phishing / Security Awareness Training (SAT)
- Advanced Endpoint Protection (AEP)
- Multi-Factor Authentication (MFA)
- Web Application Firewall (WAF)

Using the US Department of Homeland Security grant to provide local governments with tools to fill cybersecurity gaps within their environments is an innovative concept. It allows smaller and budget-constrained entities across Arizona to have access to some of the best-in-class technical solutions available in the marketplace.

For more information, visit: https://aset.az.gov/local-tribal-cyberprogram

To enhance public safety, ESPAC is partnering with the Arizona Department of Public Safety, the Arizona Department of Homeland Security, the Arizona National Guard Cyber Response Team, the FBI's Cyber Crimes Task Force, and the Urban Area Security Initiative's Cybersecurity Program Coordinator in supporting the cybersecurity capabilities of the Arizona Counter Terrorism Information Center (ACTIC). Since its creation, ACTIC has worked diligently to share critical cyber threat information and combat cybersecurity threats. As Arizona's fusion center, the ACTIC recently bolstered their commitment to this critical mission by creating the Arizona Cyber Information Program (ACIP). The ACIP brings public and private entities together through its Cyber Threat Network, to collect, share, store, and correlate information about cyber

attacks and threats. With this information, entities can better prevent cyber attacks, identify malicious software, and block phishing emails. As part of ACIP, a recently launched initiative is the training of Cyber Terrorism Law Enforcement Officers (CTLOs). This program trains Terrorism Liasion Officers (TLOs) to respond to cybersecurity crimes and collect evidence for further investigation.

To further ESPAC's goals to foster innovation and enhance information sharing, the Malware Information Sharing Platform (MISP) was deployed to share Indicators of Compromise (IOCs) amongst SLTT community partners. This replaced a manual sharing process that allows threat indicators to be shared in near real time, enabling SLTTs to quickly respond to threats. MISP also feeds into the State's Security Orchestration Automation and Response (SOAR) platform, which allows for greater flexibility in responding to threats in real time by taking automatic action in various security systems.

ESPAC has also identified workforce development and the cybersecurity talent pipeline as a priority. To create opportunities for individuals looking to start their cybersecurity careers, an internship program was implemented in collaboration with higher education institutions in the state. The goal was to mentor and grow the cyber talent by funding internships at various state agencies. The success of the program has resulted in ESPAC agreeing to double its funding for interns over the next year.

However, the talent pipeline does not begin at the university level. A Speaker's Bureau was developed to present on cyber careers and cyber best practices to K-12 educational partners. The COVID pandemic presented many challenges to under-resourced schools in the state, but it also presented an opportunity for ESPAC to reach the schools and their students remotely. Multiple interactive presentations were given to students, teachers, and parents to showcase cyber careers and programs available around the state. In conjunction with the Arizona Department of Education, ESPAC and the Enterprise Security Team are being offered as resources to school districts confronted with the unique challenges of remote device management and cyber hygiene.

IMPACT

In April 2021, Arizona Governor Doug Ducey announced State Chief Information Security Officer (CISO) Tim Roemer as the newly appointed Director at the Arizona Department of Homeland Security (AZDOHS) while also maintaining his position as State CISO in a dual role. Governor Ducey declared that "Cybersecurity is homeland security — that's why I'm looking forward to moving Arizona's critical cyber mission to the Department of Homeland Security." Subsequently, the ADOA Enterprise Security Team would also move to AZDOHS for even

greater statewide cybersecurity collaboration. Transitioning the Enterprise Security Team to the cabinet level has resulted in greater buy-in for cybersecurity across the state.

The expanded resources from AZDOHS and ongoing support directly from the Governor's Office will ensure that the State of Arizona continues to be prepared and equipped to handle threats in the cyber landscape.

REFERENCE MATERIAL