2018 Arizona NASCIO Award Nomination

Credit-Scoring Cyber Risk Management to Reduce Vulnerabilities and Strengthen Statewide Cybersecurity Posture

Category: Cybersecurity
Project Initiated: Enterprise-wide roll-out began: month after December 2015
Project Completed: Dec 31, 2017

Nomination submitted by:
Morgan Reed, CIO, State of Arizona
Mike Lettman, Chief Information Security Officer (CISO), head of Security, Privacy and Risk for the Arizona Strategic Enterprise Technology (ASET) Office of the State of Arizona Department of Administration Technology (ADOA-ASET)

Contact:
Megan Rose, Assistant Director
Statewide Communications, Arizona Department of Administration (ADOA)
100 North 15th Avenue, Suite 402, Phoenix, AZ 85007
Office: 1-602-542-1681
Mobile: 1-602-826-5406
Email: megan.rose@azdoa.gov
Websites:
https://doa.az.gov/
https://aset.az.gov

EXECUTIVE SUMMARY

Arizona is the the sixth largest and the 14th most populous of the 50 United States, with over 7 million residents. In alignment with the strategic missions of state agencies, the Arizona Strategic Enterprise Technology (ASET) office within the State of Arizona Department of Administration Technology (ADOA-ASET) is responsible for developing and executing statewide information technology (IT) strategy and providing services and infrastructure to ensure the continuity of mission critical and essential systems and initiatives for the State of Arizona including Digital Government, the Health Information Exchange, 911, state telecommunications, data network, data centers, website hosting and servers, PCs, laptops, cloud applications, security and disaster recovery. The goal of ADOA-ASET is to transform Arizona into a nationwide leader of advanced IT strategies, methodologies, services and business processes. Arizona currently has 133 agencies, boards and commissions with 32,000 employees using over 100,000 IT assets.

The State of Arizona is a federated state, and prior to this project, not many of the 133 agencies communicated with one other or even knew who the other IT managers were. From a statewide perspective, it was impossible to identify what the biggest security issues were, let alone plan how to protect against them. Nobody seemed to know what the threats were, what attackers were doing, where they were vulnerable, and there were no metrics gathered or retained. The state lacked visibility into its vulnerabilities and cyber threat risk.

Two breaches in South Carolina and Utah were a wake-up call, and the ADOA-ASET team wanted to be sure that Arizona wasn't making the same mistakes, leaving its statewide systems vulnerable. The project was budgeted to protect Arizona, to find a way to get visibility across all state agencies to identify where they were at risk and what critical IT assets might be impacted. ADOA-ASET sought and tested solutions and found a unique cloud-based platform from RiskSense that would protect Arizona against cyber attacks through broad and in-depth visibility into the state's IT infrastructure. The RiskSense cyber risk scoring system from 350-850 not only reveals where they are vulnerable and assesses risk against asset criticality, but the unique scoring system enables standardized, easily understandable communication of risks and priorities across agencies, boards and commissions.

There were three main goals for this project:

1. Gain statewide visibility into security vulnerabilities and risk and understand where to focus limited resources to achieve the greatest results in the shortest time frame to ensure Arizona's IT infrastructure was well protected against cyber threats.
2. Achieve and sustain a minimum score of 700 across all 133 state agencies, boards and commissions, an accomplishment no enterprise of AZ state's size had yet achieved.
3. The third goal, which is currently in process, is to increase all agencies to 725 or better

CONCEPT

The concept of using credit scores to improve cyber security risk is simple to understand and communicate. For instance, a credit score of 700 is good with only 5-8% experiencing issues. A cyber risk score of 700 is similarly good, indicating the organization has instituted effective vulnerability management and mitigation processes. The main components that impact an organization's cyber risk score are:

1. Effective patch management
2. Effective configuration management
3. Secure coding

To score in the 775-850 range, organizations must have developed a mature cyber risk management program where they not only routinely patch software, but also firmware, application infrastructure, Linux servers, etc.

The first goal of ADOA-ASET was to gain statewide visibility into security vulnerabilities and risk, to understand what was being attacked and how, and how to address the security gaps and vulnerabilities with limited resources. Arizona has a broad attack surface that spans the network, endpoints, applications, cloud services, mobile devices, and even IoT.

They deployed the RiskSense platform, which ingests information from Arizona's existing security investments, including network, application and database scanners, configuration management systems, etc., along with external threat data from its crawlers on exploits, malware, threat actors, reputational intelligence, from U.S. and global NVDs and vendor sites, and proprietary intelligence from its security research team that have deep knowledge from defending critical networks against the world's most dangerous cyber adversaries. RiskSense founders collaborated with the U.S. Department of Defense and U.S. Intelligence Community, developed Computational Analysis of Cyber Terrorism against the U.S. (CACTUS), Support Vectors Intrusion Detection, Behavior Risk Analysis of Vicious Executables (BRAVE), and the Strike Team Program. RiskSense takes an "attacker's view" of the entire attack surface. It correlates and contextualizes the internal and external information and evaluates asset criticality to identify imminent cyber risks and prioritize remediation.

RiskSense provides the ADOA-ASET team with a statewide credit score and credit scores for each agency, board and commission. Through a centralized, cloud-based enterprise dashboard, ADOA-ASET can drill down and communicate with the over 850 people using the RiskSense platform. ADOA-ASET management can also communicate the State's cyber risk posture using cyber risk scores, which the State's Governor and Legislators can readily comprehend.

ADOA-ASET has established standardized, disciplined and continuous workflow using this real-time cyber risk visibility to first address external, critical and then moderate vulnerabilities, through patches, configurations or mitigating controls. RiskSense cross-checks remediation efforts with vulnerability persistence analysis to ensure that applied patches, configurations and/or mitigating controls are effective. Since new vulnerabilities arise all the time, this process is continuous and ongoing.

SIGNIFICANCE

When the RiskSense Platform was first implemented, agency staff were given on-site training. The team wanted to make sure that every agency was trained and comfortable. Since then, cyber hygiene has much improved through continuous visibility into vulnerabilities for every single one of the 100K assets across the state, every day for every business unit, department, agency, as well as a broad statewide view. Arizona has gone from an initial poor score of 638 to over 700 today, with 25 agencies scoring in the excellent range above 800. One agency started with a score of 568 improved their score to 762 within 60 days.

Agencies that are not doing as well are easily identified and ADOA-ASET ensures that they receive training and/or resources and cross-training from successful agencies to improve their scores. It has been challenging to get all agencies above 700, as some are quite small, others have a lot of remote workers with devices that dock every so often, introducing potential security issues and making it difficult to schedule patches and upgrades.

On average, ADOA experiences 200 brute force attempts and 500 Trojan attacks per day; 35,000 malware attacks and 500 SQL injection attacks per month. ADOA-ASET now has the right information to identify security gaps and vulnerabilities and focus remediation efforts. On a system this large, there can be millions of vulnerabilities that need fixing across the State; however, the intelligence ADOA-ASET now has reveals optimal ways to achieve the greatest “bang for the buck”. It might show that if 15 vulnerabilities were fixed/patched on 50 assets it would eliminate cyber risk. The problem is no longer overwhelming.

In fact, Arizona now has much lower remediation costs, shorter time-to-remediation with a 45-day maximum on addressing patches. This means there is a much smaller window of opportunity for hackers to exploit vulnerabilities, which has significantly lowered the risk of cyber attack.

Arizona is now highly resilient to cyber threats. For example, RiskSense alerted ADOA-ASET to the Apache Struts vulnerability (which was used in several high profile breaches including Equifax) as being a critical threat and pinpointed which systems were affected. In only one day, ADOA-ASET was able to remediate all 33 machines that were vulnerable and the State wasn’t affected at all by the widespread attack. A similar situation arose with WannaCry and Arizona was not impacted.

Credit-scoring cyber risk management has enabled ADOA-ASET to reduce vulnerabilities and strengthen statewide cybersecurity posture. It has also helped communication with top level executives. The score allows executives to easily understand the State’s current risk position and trends over time.

IMPACT

Cyber attackers have an asymmetric advantage. They don't need to know everything on a network, as they only need to find one way in. Five people with 10 laptops could take down an entire nation. Defenders on the other hand must be able to find all possible infiltration points. In a network the size of Arizona, this is not a humanly possible task. The RiskSense platform's human assisted machine learning intelligence provides a single pane of glass whereby the ADOA-ASET team and the IT staff within the State's many agencies, boards and commissions can even the playing field with attackers and assure that Arizona's IT infrastructure is well protected against cyber threats.

As a result of this project, the ADOA-ASET team is able to determine in real-time:

- Whether business critical assets are at risk
- Which assets have vulnerabilities and whether they can be exploited
- How cyber adversaries are attacking in the wild and whether Arizona is vulnerable
- Best course of action for remediation efforts to address critical assets first

The ADOA-ASET team remains dedicated to maintaining visibility into cyber risk and improving security posture. The team was able to achieve its goal and sustain a minimum score of 700 across all 133 state agencies, boards and commissions. Currently, the team is working to get the score up to 725.

Using this project's successful outcome to further benefit the State, the ADOA-ASET team is currently attempting to leverage these cyber risk scores to demonstrate cyber risk management effectiveness to obtain lower premiums on the cyber insurance that is required for federated states.