State of Nevada

NASCIO 2019 State IT Recognition Awards Submission

Title: **A Community Approach to Cyber Security**

Category: Cybersecurity

State: Nevada

Contact: Michael Dietrich, Chief Information Officer
Phone: (775) 684-5849
Email: MDietrich@admin.nv.gov

Project Initiation and Completion Dates:
May 2017 – December 2018

Executive Summary

It's no surprise that NASCIO's 2019 State CIO Top 10 Priorities list ranks "Security and Risk Management" at the top, as it has since 2014. One only has to look at the number and impact of the high-profile ransomware attacks that occurred at the state/local level over the past year to see that State and local agencies are under constant threat. As the guardians of significant amounts of citizen data, our agencies must be focused on protecting personally identifiable information (PII) and the overall privacy of our constituents.

In addition, statewide information security programs must be broad enough to address control sets from myriad regulatory requirements, properly and effectively secure a wide-range of data types, support the business processes and work flows of dozens of agencies (each with their own mandates and requirements), and adapt to the changes in direction and priorities that a regular election cycle may bring. With all that said, the State of Nevada, along with most state agencies, is facing this challenge with limited resources – both from a personnel and capability perspective.

As a result, the State of Nevada moved to a new approach to information security by building collaborative partnerships, both within the state government and beyond, and transitioning to a managed security services program in conjunction with industry. Our focus was on open, clear communications and the use of existing tools to support ongoing needs, which has resulted in a more secure environment across the state.

Project Narrative

Concept

As noted, information security programs in state governments are required to overcome substantial, unique difficulties, in addition to addressing similar challenges faced by their counterparts in the private sector.

Statewide public-sector information security programs must be broad enough to address control sets from myriad regulatory requirements, properly and effectively secure a wide-range of data types, support the business processes and work flows of dozens of agencies (each with their own mandates and requirements), and adapt to the changes in direction and priority that a regular election cycle may bring. The cornerstone of the State of Nevada's approach to information security is the building of collaborative partnerships, both within the state government and beyond. It's focused on open, clear communications and the use of existing tools to support ongoing needs.

We run a decentralized information security model to empower each agency to operate independently. This model is coordinated and supported by the State's chief information security officer (CISO), whose Office of Information Security provides a core set of enterprisewide security services. Each agency, however, is guided by its own information security officer (ISO) whose sole focus is to secure that specific agency. In this endeavor, ISOs benefit from the core set of security services provided by the state CISO office. The state CISO chairs a statewide committee that coordinates security activities. This committee, which includes all agency ISOs, provides a collaboration forum for what the CISO and deputy CISO call their 'state security community.'

As part of its commitment to the state security community, the Office of Information Security delivers a core set of enterprisewide services that are broadly applicable to support the community's range of needs. All the standards roll up to, and get their authority from, one consolidated policy. In general, those standards are aimed at a baseline to enable everyone to comply. State security standards are, of course, constantly evolving. Standards are revised in a subcommittee and then brought back to the main committee where everyone weighs in and votes.

All incident notifications from external SOCs go through the Office of Information Security. They are reviewed, assessed for validity, and forwarded to the appropriate agency ISO. Additionally, the team empowers each ISO to increase their knowledge base while avoiding unnecessary duplication, such as helping them interpret the notification or provide additional logs or analysis. Reports correlate incidents to make sure the same incident is not reported multiple times.

Significance

Collaboration and communication are key. The community approach relies on an active and collaborative partnership that strengthens and supports the community. This includes when

making critical decisions around the adoption of new technologies and services. When the Office of Information Security initiates a project, it asks the security community for volunteers, especially among people who are already involved in a particular technology, or who have a very strong need for that type of a service or capability. A task force is formed to identify common requirements and a core set of business needs. Then the team works together to evaluate and select the products.

In this process, if an agency is considering a technology that benefits the state as a whole, it will be elevated from an agency purchase to a statewide purchase in order to get the economies of scale. This helps agencies that don't have the resources like some of the larger, better-funded agencies, and gets them tools that otherwise would be beyond their reach.

Agencies across the state benefit from the Office of Information Security, which not only provides services but also shares information, acting as subject matter experts. It's beneficial to the community as a whole to have ISOs that are willing to share with other ISOs, and to collaborate with each other on projects or issues that are bigger than one individual agency can handle, or that impact more than one agency. There's a strong sense that the security community approach in Nevada works because no one is forcing anyone else's hand in these relationships. It is approached as a mutually beneficial relationship.

By working hand-in-hand with their key cyber security partners—and by not being reluctant to ask for help with their investigations—Nevada is leveraging all its available resources. The Office of Information Security understands that if it contains all the investigative effort, it creates silos and cuts itself off from the resources and insights of others. It is much better to leverage the expertise of others, whether another agency or a security vendor.

The Office of Information Security uses both in-house and external resources to take in all different layers of intelligence, data, and analysis and develop processes that correlate it all into actionable intelligence. For example, this includes network logs, all traffic through our network devices, as well as logs from our critical infrastructure components. That's raw data from billions of records—more than our staff could possibly process. Even if we had enough staff, we would need to put them through advanced training and have them onsite 24x7x365—and we would still need to make significant investments in hardware, software and analytics capabilities. It is just not feasible.

As such, the state adopted a managed service partnership as well. The Office of Information Security has its internal systems that are monitoring for anomalies and inappropriate traffic, which are blocked by their own network defenses. These notifications are collected in a repository; then various scripts look at the data, sort it into different buckets, and identify what needs further analysis. In fact, automation is key to how the Office of Information Security does so much with such a small team. Scripts are constantly taking care of fairly simple but necessary and time-intensive tasks, enabling team members to do the work of five or six people. Coupled with the application of specific technologies, and vendors working in unison, the team is able to punch well above its weight in the fight against cyber threats.

When the Office of Information Security detects a vulnerability to an urgent, large-scale attack, it quickly sends individual notifications to agencies statewide with direction on how to remediate, and they do this agency by agency.

Impact

As we all know, the results associated with a cyber security initiative are often hard to measure, so the best way I know how is to provide some distinct examples of how open communication and a willingness to share information made all the difference.

- In late 2018 a spate of emails containing bomb threats were received across the United States. Normally in Nevada, bomb threats go to the Department of Public Safety or Threat Analysis Center. However, the Office of Information Security got looped in by various agency security officers because the threats were coming in by email. The team immediately engaged with a unit within their Department of Public Safety—the Office of Cyber Defense Coordination—and with the Nevada Threat Analysis Center. As a result, the team was able to determine quickly that the bomb threats were hoaxes. By reaching out and partnering with other agencies, the Office of Information Security was able to get to the root of the issue and send out an all-clear within a couple hours. If they had kept the investigation internal, they would've been spinning their wheels for quite a while and wasting a lot of cycles trying to determine if the threat was legitimate. To those unfamiliar with the machinations of information security within the public sector, this scenario may not seem so out of the ordinary; however, many states don't have this culture of trust and communication—and therefore they don't have the kind of security that's present within the State of Nevada.

- Another prime example was in combating WannaCry and NotPetya. The team successfully fought these two ransomware attacks that crippled many public sector organizations across the globe. As soon as the Office of Information Security received the first indications of what was going on, they started doing custom scans of all the systems, identifying which specific agencies and systems had a potential exposure. Thanks to the layered security approach, only eight systems across the entire state were infected. One was a misconfigured workstation that wasn't getting updated, and the other seven resided in an agency that was not taking advantage of the state's enterprise security offerings. That agency is currently working out the logistics necessary to migrate onto the enterprise platform.

Too often, information security efforts focus on implementing technology rather than engaging with people. This collaborative approach to cyber security in Nevada, led by the Office of Information Security, is a unique effort to help curtail threats across the state, and fully aligns with the state's overall Road to Unity strategy of collaborative IT planning, management and service delivery. Working in a collaborative, communicative environment with our agencies, as well as our industry partners, is a model that should be considered by states across the U.S.