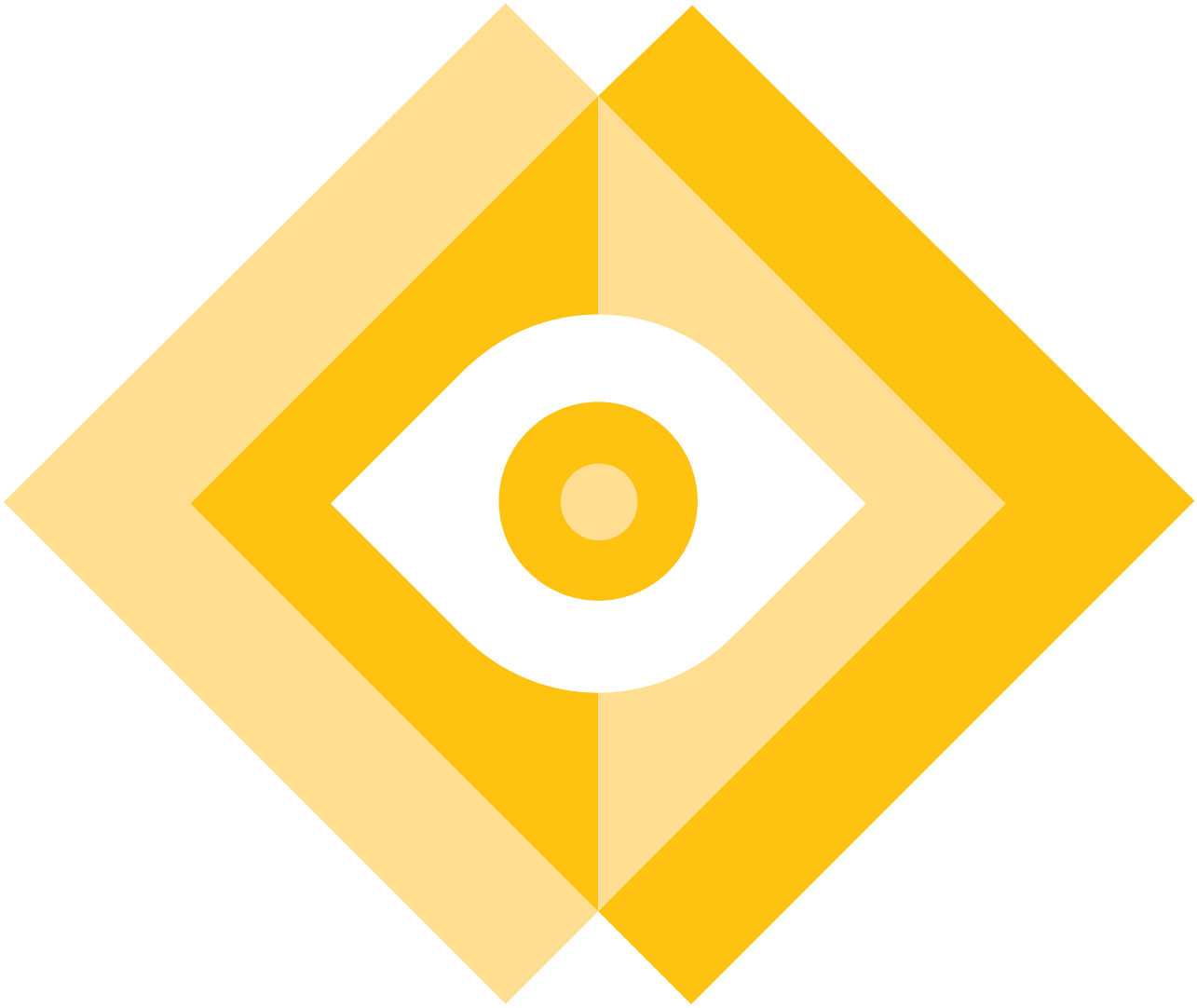

State of Nevada Addresses Information Security Challenges through Security Community Approach

WHITE PAPER

Participants:

Bob Dehnhardt, State Chief Information Security Officer
Jenet Hensley, Deputy CISO

State of Nevada, Department of Administration, Office of Information Security

Symantec™

Introduction

Information security programs in the public sector are required to overcome substantial, unique difficulties, in addition to addressing those same challenges faced by their counterparts in the private sector. Statewide public-sector information security programs must be broad enough to address controls 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.

The State runs 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 agency alone. 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.'

Statewide Security Standards

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.

As Bob Dehnhardt, State CISO, spells out, "We have one consolidated policy that all the standards roll up to and get their authority from. In general, those standards are aimed at a baseline." As Dehnhardt and the OIS team are only too aware, different agencies have different needs, so they try to set the standards at a level where everyone can comply. "There are always going to be exceptions, continues Dehnhardt. "We want to positively impact security, but not make it so onerous that smaller agencies are overburdened."

Naturally, some agencies find it necessary to meet a higher standard—they may need to enforce more rigorous policies or invest in additional IT security resources. But if particular agencies find the baseline standard is sufficient, they're not required to go any further, which is a blessing when resources are stretched thin.

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. As the committee chair, Dehnhardt oversees the committee's approval, and then takes it to his boss (the CIO) for approval.

Core Enterprisewide Services

Jenet Hensley, Deputy CISO, describes services that lessen the burden on ISOs. "Each person [on the team] has a lead role in a separate and distinct area. We cross-train to make sure we have coverage when people are sick or on vacation. All incident notifications from external SOCs go through our office," says Hensley. "We review them, assess their validity, and forward them to the appropriate agency ISO."

Additionally, the team does its utmost to empower each ISO to increase their knowledge base while avoiding unnecessary duplication. "If an agency ISO needs technical support, we'll provide it," says Hensley. "We may help them interpret the notification or provide additional logs or even analyze those logs—whether from Symantec, MS-ISAC, Albert sensors, FBI InfraGard association, the DHS Homeland Security Information Network or other sources. We correlate incidents with our internal reports to make sure we don't double report the same incident coming in from two different sources."

Collaboration and Communication Are Key

The community approach relies on an active and collaborative partnership. As Hensley explains, "We don't keep things secret like we're the only ones who can have the information about

the threats. We treat our security community like our extended family; that's what builds this close working relationship." Through their committee, Hensley and Dehnhardt work to strengthen and support the community.

Dehnhardt relates an example 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 ISOs because the threats were coming in by email. Dehnhardt and 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 pretty quickly that the bomb threats were hoaxes.

By reaching out and partnering with other agencies, Dehnhardt says, "We were able to get to the root of this pretty quickly and send out an all-clear within a couple hours. If we had kept the investigation internal to our unit, we would've been spinning our wheels for quite a while and wasting a lot of cycles trying to determine if it 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.

Gathering Consensus on Technology Adoption

Dehnhardt and Hensley are similarly collaborative when making critical decisions around the adoption of new technologies and services. Hensley elaborates: "When our office initiates the project, Bob and I ask 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. We form a task force to identify our common requirements, a core set of business needs that will be supported by that. Then we work together as a team to evaluate and select the products."

Once the decision has been made to move forward with a particular technology or service, Dehnhardt steps back into the fray and negotiates the agreement with selected product vendors. However, not everything begins with the CISO office: "I gladly steal, with attribution, good ideas coming from the agencies," says Dehnhardt. "If an agency is considering a technology I feel would benefit the state as a whole, I'll elevate it from an agency purchase to a statewide purchase and get the economies of scale. This really 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."

Mutually-beneficial Collaboration

The agencies benefit from an Office of Information Security that's providing services they need, and sharing information and acting as subject matter experts when they have problems. "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," says Dehnhardt.

There's a strong sense that the security community approach in Nevada works because no one is forcing anyone else's hands in these relationships. Dehnhardt and team don't simply issue diktats from their elevated positions, but rather they seek to cooperate and collaborate.

"We've been successful because we don't force, dictate, or legislate our security community to do anything," says Dehnhardt. "We approach it as a mutually beneficial relationship and we are willing to reach out and share information and to ask questions and offer solutions."

While there might be some benefit in creating a dotted line reporting structure between the CISO and the agency ISOs, Dehnhardt feels that's a double-edged sword. There's a distinct relationship between the CISO's engagement and communication style, and the level of participation: The more autocratic, the less inclined people are to participate.

Dehnhardt says, “Putting our relationships into policy would probably cause some willing participants to take a step back and say, ‘I’m not sure I want to participate in this formal process.’ You build what we’ve got through the right attitudes, through openness in communications and a willingness to collaborate. I just don’t think you can really legislate something like that.” No one’s forcing anything down anyone’s throat, and so the teams actually want to work together.

Hensley wholeheartedly agrees, “From my perspective, formalizing the relationship would be a serious detriment. Yes, we have to continually reinvent ourselves to be responsive to our agency partners. Why? Because technology changes, the attacks change, the business needs change, all of which drives yet more changes in security requirements.”

Naturally, this voluntary approach carries with it the risk that agencies might not engage. Dehnhardt’s approach is to keep the lines of communication open and reinforce the positive aspects of cooperation. “If things go sideways for an agency that hasn’t actively engaged, we’ll still support them however we can, and help mitigate the problems going forward. But at some point, they may have to stand alone if they choose not to take advantage of the services we offer.”

Partnering with Security Vendors

By working hand-in-hand with their key cyber security partners, by not being reluctant to ask for help with their investigations, Dehnhardt and Hensley have been able to leverage all the resources available to them.

Dehnhardt elaborates: “We’ve thrown around the term partnership an awful lot, but I think that’s really the key to all of this. We realize none of us knows everything. If my office contained all the investigative effort, we’d be putting ourselves in silos, cut off from resources and insights. Much better to reach out and find out what others know, whether it’s another agency or a security vendor like Symantec.”

Actionable Intelligence and Layered Security Defenses

Comprehensive security these days relies on an integrated approach to cyber defense. So it’s of paramount importance that a CISO can take in all those different layers of intelligence, data, and analysis and develop processes that correlate it all into actionable intelligence.

As Hensley explains, those processes are many and varied: “Some of it is review and analysis by the team, some of it we’ve automated with custom, in-house tools, some of it by taking advantage of the tools that we have. Symantec is our data cruncher. Symantec gets all our network logs, all traffic through our network devices, as well as logs from our critical infrastructure, such as Active Directory and DNS servers. That’s raw data, billions of records. We don’t have enough staff to process all those raw logs ourselves.”

While Dehnhardt isn’t a huge fan of outsourcing, he acknowledges that using a managed service “just makes sense. Trying to compile all the hardware and software you need, all the analytics, getting staff in place, training them up to be true security experts, having them onsite 24x7x365. It just makes so much more sense going outsourced for that.”

But it isn’t as simple as just handing over responsibilities to a vendor. The State CISO also has internal systems that are monitoring for anomalies and inappropriate traffic, which are blocked by their network defenses. “If we know of a particular set of command and control servers, or malicious content servers, or certain sites our state workers shouldn’t visit, our systems block access and automatically notify our group,” Hensley relates. “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.

Combating WannaCry and NotPetya

Hensley shares some interesting context on how the team successfully fought two recent ransomware attacks that crippled many public sector organizations across the globe. "When choosing products, if you look at security holistically you can create some interesting synergies. Remember the WannaCry and NotPetya attacks? That was actually quite a success for us. As soon as we got the first indications of what was going on, we started doing custom scans of all the systems, identifying which specific agencies and systems had a potential exposure. That really helped us contain our risk."

"Thanks to our layered security approach, only eight systems across the entire state enterprise were infected," Hensley continues. "One was a misconfigured workstation that wasn't getting updated. The other seven resided in an agency that was not taking advantage of our enterprise security offerings. When we detect a vulnerability to an urgent, large-scale attack, we quickly send individual notifications. 'Hey ISO at agency X, you have seven systems with this vulnerability. This is their IP addresses and names. We really advise you patch them immediately.' We do that agency by agency."

Dealing with the Cloud Generation

Dehnhardt's two biggest current concerns relate to cloud security and the mobile workforce. "The new technology paradigm in my experience is not well understood at this point. There's a distinct knowledge gap around how to properly secure a cloud environment. There's a knowledge gap around how to completely protect an endpoint that's been taken beyond your perimeter and then brought back in."

Dehnhardt's next major concern addresses arguably the greatest challenge facing CISOs across the globe right now: human nature. "These days, as attacks focus more on users rather than the technology, I'm emphasizing multifactor authentication and user security awareness training."

As for advising others in a similar position, Hensley sees open communications, inclusivity, and keeping an open mind as key. "As we committed to this vision of a collaborative partnership, people have started to rethink their lack of involvement. We have had agencies come to the table in the last couple of years that ten years ago were flatly opposed to it."

"If I had to give advice, I'd say be willing to fail, be willing for it to not work right off the bat," says Dehnhardt. "Because it won't. It's going to take time to build the trust, openness, and willingness you need. Just move it a step forward each time."

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

19D213249_wp_State_of_Nevada_EN