2015 NASCIO RECOGNITION AWARD NOMINATION

Name of State Agency:

- State of South Carolina
  - *Division of Information Security (DIS)*
  - *Enterprise Privacy Office (EPO)*
  - *Human Resources Division (HRD)*

Project Managers:

- Marcos Vieyra, Chief Information Security Officer, DIS
- Alex White, Deputy Chief Privacy Officer, EPO
- Michele Perrick, Deputy Chief Privacy Officer, EPO
- Sam Wilkins, Director, HRD

Name of Project Executive Sponsors:

- Marcia Adams, Director, Budget & Control Board

Project Initiated:

- September 2013

Project Completed:

- April 2015

EXECUTIVE SUMMARY

Recently major data breaches have hit the news with fearful regularity, affecting entities from private sector to government. The States of Utah and South Carolina, the Department of Defense, and Home Depot have all been in the spotlight, to name a few. In fact, according to the DataLoss DB (database), data breach incidents reached an all-time high in 2012[1]. As breaches continue to escalate in complexity and severity, government agencies and private sector organizations scramble to improve their information security (InfoSec) and Privacy practices, such as network segmentation, better access controls, and regular vulnerability assessments. Additionally, state governments are increasingly looking to employ initiatives that strengthen their InfoSec and Privacy workforce. The 2014 Deloitte_NASCIO Cybersecurity Study, titled "Talent Crisis," highlights the challenge as key, based on input from 49 states responding to a survey. A well-developed, skilled, and cyber-aware workforce at all levels in the organization can better protect systems, networks and data, helping to proactively address future threats in this ever-changing environment.

The State of South Carolina (State) announced data breaches that occurred between August and September of 2012[2]. Under the leadership of Budget and Control Board Director Marcia Adams, the Division of Information Security (DIS) has been driving the development, implementation, and adoption of a Statewide InfoSec and Privacy program. The State's Chief Information Security Officer (CISO), Marcos Vieyra, in collaboration with the Enterprise Privacy Office (EPO) and Human Resources Division (HRD), is enacting a large-scale response with the goal of securing the State's information assets and protecting its citizens. The State hired Deloitte & Touche LLP to assist with initial assessments and design of the InfoSec program. An important aspect of this program is the development and execution of a customized plan to strengthen the State's InfoSec and Privacy workforce, which helps prevent future breaches. DIS, EPO and HRD worked aggressively to implement a Professional Development Program (PDP) as a complement to the technology and process components of security and privacy.

Through deployment of the InfoSec and Privacy PDP, the State established the foundation for a strong technical and cyber-aware workforce. The PDP helps the State more strategically hire, develop and retain the critical skills it needs to better protect citizen information and data.

BUSINESS PROBLEM AND SOLUTION DESCRIPTION

The September 2012 data breach occurred when an agency employee opened a phishing email which provided the hacker access to the agency's data systems, affecting roughly 3.6 million State citizens. After the breach, several top-level government officials supported strategic initiatives to remedy the breach. The State provided tools to help affected citizens, consisting mostly of credit monitoring services and continued communications on efforts taken to remedy the breach. This incident resulted in significant

[1] http://datalossdb.org/statistics
[2] http://www.eweek.com/security/massive-data-breach-hits-south-carolina-state-tax-system

monetary costs; over $12 million for credit monitoring services alone[3] and additional costs implementing new security controls and hiring third parties to help prevent future incidents. The State also dedicated a portion of the workforce to remedy the breach, removing these individuals from other job responsibilities and potentially slowing down essential operations. Additional non-monetary impacts, including loss of stakeholder confidence and disruption to operations, can be just as damaging to the State as the $12 million price tag for credit monitoring.

The State examined its own security policies and mandated that all Cabinet agencies use the State's monitoring services. Additionally, a security risk assessment was conducted and determined that one of the strategic focus areas moving forward needed to directly address the InfoSec and Privacy Workforce. The PDP was hence established by DIS, EPO and HRD to take a holistic approach to developing the "people" component of InfoSec and Privacy for the State, and consists of the following:

- Statewide InfoSec and Privacy skills assessment survey
- Design of new InfoSec and Privacy talent development initiatives such as:
    - Modernization of the IT classification, including increased pay bands
    - Development of a technical competency model, position descriptions and a career path
    - Development of a training framework, tied to competencies and position descriptions
- Statewide change management workshops to release the PDP to end users and encourage enterprise-wide adoption

The 2014 Deloitte_NASCIO Cybersecurity Study found that nearly 92 percent of states said existing salary ranges and pay grades presented a challenge when attracting and retaining employees.[4] In fact, nine out of ten respondents said salary was the biggest challenge when attracting talent.[5] The State of SC's IT classification modernization not only introduces new classes dedicated to InfoSec and Privacy positions for more accurate classification, but also introduces higher pay bands, providing State agencies the ability to better compensate their employees and become more competitive with salary expectations, budget allowing. Furthermore, it was apparent that the lack of a clear career path and adequately documented expectations further complicate recruitment and retention processes for InfoSec and Privacy employees. In response, the State developed 30 distinct InfoSec and Privacy position descriptions to help define expectations, and coupled those with competitive non-salary benefits to their employees, such as formal trainings tied back to technical competencies and expectations in order to help employees take ownership of their development. The PDP also offers a new and forward-thinking career path model to provide visibility into various options (both managerial and technical) available to InfoSec and Privacy employees, with added pay bands along the technical career path for increased retention.

The development and deployment of these initiatives helps the State strategically hire, onboard, develop and retain its critical InfoSec and Privacy workforce in the face of the talent hurdles this industry faces.

---

[3] http://www.usatoday.com/story/news/nation/2013/02/27/hacker-south-carolina/1951719/

[4] http://www.govtech.com/security/Hiring-Cybersecurity-Staff-Is-Hard-for-States.html

[5] 2014 Deloitte NASCIO Cybersecurity Study

SIGNIFICANCE

The State's deployment of the InfoSec and Privacy PDP aligns to the State's top leadership cybersecurity priorities[6], improves the InfoSec and Privacy operations of the State, and provides agencies with the appropriate tools to increase their security posture. Further, agencies can now better hire, train, and retain a knowledgeable workforce through use of the PDP artifacts.

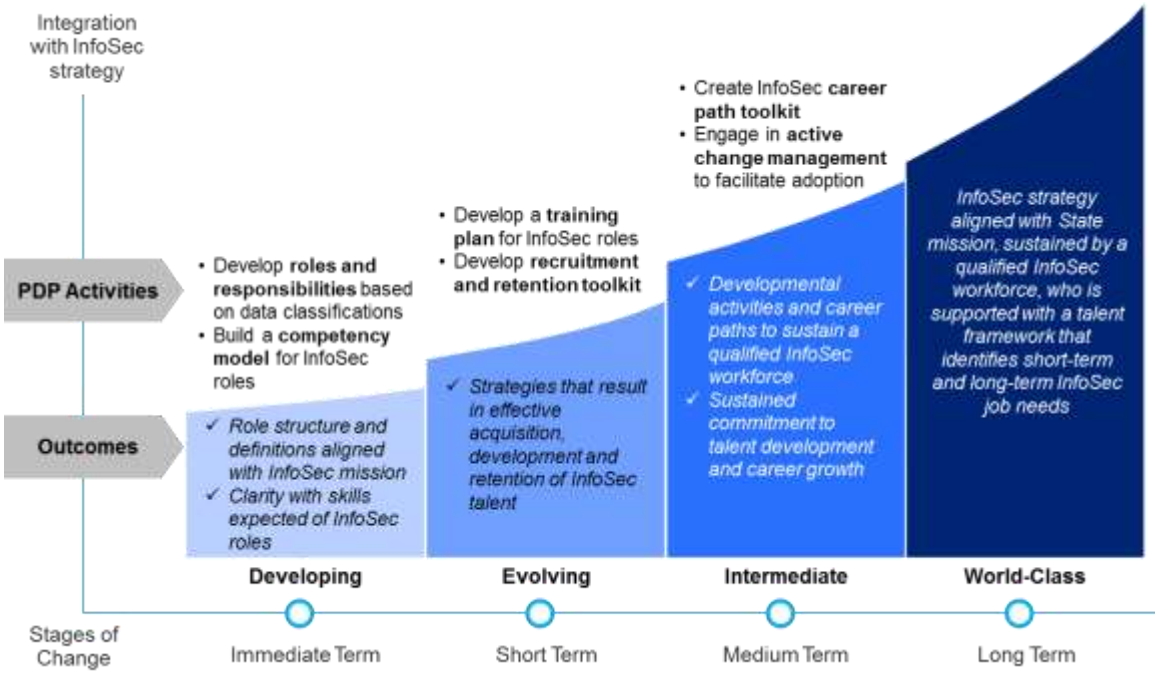
The new competency model outlines requisite knowledge, skills, and abilities (KSAs) needed to fulfill the State's InfoSec and Privacy positions and serves as the foundational element for all new InfoSec and Privacy talent practices. Agencies use these competencies to fulfill the expected roles and responsibilities, as needed, to help support the execution of and compliance with State InfoSec and Privacy programs. Position descriptions build off the competency model by featuring new positions that can perform the roles and responsibilities necessary to support InfoSec and Privacy for State agencies. These position descriptions are aligned with a newly defined and modernized pay structure and classification model. A training framework illustrates InfoSec and Privacy training opportunities to encourage workforce development and retention, and links directly to the new career path model to inform InfoSec and Privacy workforce development planning, evaluations of personnel strengths and areas for improvement, and career progression conversations.

With these tools, agencies have greater control over their InfoSec and Privacy workforce acquisition and effectiveness, helping to combat several of the statistics mentioned in countless cybersecurity organizational studies over the years. The State of SC is at the forefront of government in the design and implementation of talent solutions for one of the emerging but arguably most critical workforce segments in today's digital age.

BENEFIT OF THE PROJECT

PDP artifacts are targeted to constituent groups such as HR Directors, Agency Heads, InfoSec and Privacy Personnel, and State employees interested in joining the InfoSec and Privacy workforce. Each activity, as outlined in the figure below, has helped DIS and EPO address InfoSec and Privacy workforce gaps, and move along the change curve toward a world-class program.

[6] http://www.usatoday.com/story/news/nation/2013/02/27/hacker-south-carolina/1951719/



Over the course of almost two years, the State dedicated resources to the immediate, short and medium term stages of change. In April and May 2015, DIS, EPO, and HRD engaged stakeholders directly in this effort, by inviting HR Directors, InfoSec Liaisons, Privacy Liaisons, and IT Directors across all agencies to PDP workshops so that they can learn about the program, how it helps them close talent gaps, and for end users, how it helps them manage their own careers. Over 110 HR and 80 InfoSec, Privacy, and IT participants attended the workshops, showing the incredible state-wide interest in these types of workforce solutions. Subsequent to the workshops, agencies are already actively adopting artifacts, such as the Position Descriptions, to their new job postings and to aid in proactive performance management. The acceptance of the PDP and its artifacts is significant because State agencies are not mandated to adopt these recommendations.

Marcos Vieyra, DIS's Chief Information Security Officer, stated that "the State of South Carolina's InfoSec and Privacy program consists of three pillars: people, process, and technology. The people component is by far the most important; without people who can effectively perform InfoSec and Privacy duties, or who understand their role in the protection of State information assets, the program cannot be effective. The PDP helps make sure that the right people with the right skills can implement the necessary processes and technology. Through the deployment and continued maturation of the PDP, the State of South Carolina is at the forefront of developing a skilled InfoSec and Privacy workforce."

The PDP shows how the State is actively investing in its InfoSec and Privacy workforce through leading and unique workforce practices. The participation and adoption of this deployment have been successful to date, and as more agencies continue to mature their InfoSec and Privacy programs, they have the tools essential to hire, retrain, and better develop a skilled InfoSec and Privacy workforce. The proactive investment by the State in its people, and not just in InfoSec and Privacy processes and technology, helps it better detect and mitigate potentially costly incidents such as the one encountered in 2012.