NASCIO 2018 State IT Recognition Awards

Cybersecurity Apprenticeship Program

Category: Cybersecurity

State: Ohio

Contact:

Katrina Flory
Ohio Department of Administrative Services
Office of Information Technology
614.995.5466
Katrina.Flory@das.ohio.gov

Project Initiation: May 2016

Project Completion: September 2017

Executive Summary

The State of Ohio is working daily to fortify its' infrastructure and protect its data. Given today's environment, protecting the state's assets from cybersecurity threats is an ongoing effort that requires Ohio to be proactive and resourceful. The State of Ohio, on average, detects 10 suspicious offences per hour, or one every 6 minutes, through its security information and event management tool. The state's security capabilities work to ensure that data is protected from the endpoint to the service, securing 72,000 endpoint devices and actively scanning more than 100,000 devices for vulnerabilities. Given Ohio's significant IT security footprint, it is critical that the state be able to attract and retain IT security professionals. However, this is challenging in today's job market given the demand for these resources as well as the current salary levels. State government cannot compete with private industry in terms of compensation. According to recent Gartner research note, "the unemployment rate for cybersecurity professionals is zero."[1] In addition, Gartner advises that, "the U.S. Bureau of Labor Statistics expects that demand for cybersecurity professionals will increase 53% through 2018."[2] This data clearly indicates the need for a creative and innovative approach to filling cybersecurity roles.

The Ohio Department of Administrative Services (DAS) Office of Information Security and Privacy (OISP) supports and collaborates with internal and external agency customers to lead the creation, implementation and management of enterprise efforts for information assurance, security, privacy and risk management. In an effort to fill critical cybersecurity roles in their office, DAS OISP partnered with the DAS Office of Employee Services and the Ohio Department of Job and Family Services Apprenticeship Office of Workforce Development to develop a creative solution to this challenge. The team understood that the solution needed to balance the state's inability to match private sector salaries with the need for candidates that will make an investment in the State of Ohio as an employer. DAS OISP is interested in recruiting resources that will work to obtain the skills needed to fill Ohio's IT security needs. Leveraging the expertise of each of these areas, the team was able to identify a creative and realistic solution for Ohio – the Cybersecurity Apprenticeship Program.

The program is a brand new approach for Ohio and is already yielding results. It establishes a cybersecurity resource recruitment pipeline. The apprenticeship program allows DAS to recruit college graduates as well as those still in college. DAS also accepts applicants who are in a certification training program or professionals looking to change careers. Internal candidates are also eligible to participate. To date, DAS OISP has three cybersecurity apprentices in place. They are already working with their DAS OISP mentors to become cybersecurity professionals for the State of Ohio.

---

[1] Olyaei, Sam, Mark Coleman, Matthew T. Stamper. "Adapt Your Traditional Staffing Practices for Cybersecurity," Gartner, 2 May 2018 < https://www.gartner.com/en>.
[2] *Ibid.*

Concept

Recruiting qualified cybersecurity professionals is difficult for every organization. The deficit of experienced talent combined with the high demand for resources has driven the Ohio Department of Administrative Services (DAS) Office of Information Security and Privacy (OISP) to develop a creative solution to this challenge. Working with the DAS Office of Employee Services (OES) and the Ohio Department of Job and Family Services (JFS) Apprenticeship Office of Workforce Development, DAS OISP has developed a Cybersecurity Apprenticeship Program.

Through the new DAS program, IT security apprentices will gain experience in all of the major areas of a large cybersecurity program. The apprenticeship program allows DAS OISP to recruit college graduates, as well as those still in college. DAS OISP is also able to accept applicants who are in a certification training program, professionals looking to change careers, or those that would like to enter the IT field. The apprentices work 32-40 hours a week in four different groups within DAS OISP.

Apprentices are recruited in “cohorts” and the apprenticeships will last up to two years and be recognized nationally by the Ohio State Apprenticeship Council. All apprentices will be required to complete 2,000 on-the-job hours as well as 200 instructional credit hours through a customized learning module in DAS’ e-learning portal, Learning on Demand.

Required cybersecurity apprentice training offerings include:

- **Business Skills**: Communication, Time/Organizational Management, Conflict Management, Emotional Intelligence/Leadership, Critical Thinking / Problem Solving, Customer Service

- **Information Technology**: CompTIA Network +, CompTIA Security +, CompTIA Linux +, CompTIA Server +, CompTIA Cloud+, ITIL 2011, Certified Ethical Hacker (CEH), Systems Security Certified Practitioner (SSCP) 2015, CompTIA CSA+

Working closely with DAS OISP security staff, the apprentices will rotate through each of the following four areas:

Governance Risk and Compliance – measurement and monitoring of cybersecurity risk

Enterprise Vulnerability Management – network and application vulnerability detection and remediation

Security Engineering – operation of enterprise security tools

Security Incident Response Team – monitoring of enterprise security tools and incident response

In addition to spending three months in each of these four groups, apprentices will meet with other DAS OISP teams (e.g. State CISO, Chief Privacy Officer, Chief Security Architect, etc.) to gain a better understanding of their roles and responsibilities.

Once an apprentice has completed 2,000 work hours (approximately one year) and the 200 hours of required training, they will earn their certificate of completion for the apprenticeship program. Completion of the program will qualify them to interview for an entry level security position within DAS OISP. They may elect to be placed in one of the four security teams mentioned above for a deeper emersion into their area of interest or they may stay with DAS OISP for an additional 18 months while they are seeking job placement.

The DAS OISP apprentice requires some knowledge of information technology to assist DAS OISP staff. The detailed job description includes the following details for each of the rotation areas:

Governance Risk and Compliance

- Assists in performance of security reviews, to identify gaps in security architecture, and develop a security risk management plan
- Assists in reviewing authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network
- Assists with review of cloud service provider qualifications
- Assists in performing risk analysis (e.g., threat, vulnerability, and probability of occurrence) on new systems and applications for initial installations and major updates

Enterprise Vulnerability Management

- Assists in conducting assessments of threats and vulnerabilities; determining deviations from acceptable configurations, enterprise or local policy; assessing the level of risk and determining appropriate mitigation countermeasures in operational and nonoperational situations
- Assists in measuring the effectiveness of defense-in-depth architecture against known vulnerabilities
- Supports penetration testing on networks, systems or elements of systems
- Assists in identifying systemic security issues based on the analysis of vulnerability and configuration data
- Assists in the preparation of vulnerability reports that identify technical and procedural findings, and provides recommended remediation strategies/solutions

Security Engineering

- Assists in providing support, administration, and maintenance necessary to ensure effective and efficient information security systems

- Assists in conducting technology assessment and integration process
- Provides and supports a prototype capability and/or evaluates its utility
- Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions
- Provides guidance to customers about applicability of information systems to meet business needs
- Assists in development and in conducting system tests to evaluate compliance with specifications and requirements, by applying principles and methods for cost-effective planning, evaluation, verifying, and in validating technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.

Security Incident Response Team

- Assists in investigation of cybersecurity events related to IT systems, networks, and digital evidence
- Assists in identifying, analyzing, and mitigating threats to internal IT systems, and/or networks
- Assists in testing, maintaining, and reviewing infrastructure hardware and software that is required to effectively manage the computer network defense service provider network and resources
- Monitors network to actively remediate unauthorized activities.
- Assists in the response to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats.
- Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security

Other duties as assigned, including but not limited to:

- Completes specific training requirements
- Keeps up-to-date on current threats and vulnerabilities
- Monitors changes in cybersecurity related policy, regulation, and law

Significance

The Cybersecurity Apprenticeship Program is in direct alignment with the spirit of Governor John Kasich's Workforce Transformation initiative. The overall goal of Workforce Transformation is, "To grow Ohio's economy by developing a skilled and productive workforce, promoting effective training programs, and connecting Ohio employers with qualified workers." This new program is allowing interested parties the opportunity to work alongside seasoned IT security professionals who will mentor them in a variety of important cybersecurity roles and the state is also providing access to valuable training resources. The ultimate goal is to provide a long-term career path for cybersecurity apprentices within state government. The program is broad in scope, allowing individuals to participate who are in various stages of their career, including,

college graduates, those still in college, applicants who are in a certification training program, professionals looking to change careers, and internal state government candidates.

This program is also directly related to the number one item in NASCIO's State CIO Top Ten Priorities for 2018 - Security and Risk Management. The program represents a foundational element to developing, implementing, and maintaining effective statewide security capabilities.

Over the years, DAS has leveraged college internships as a potential avenue for obtaining resources. However, this new program is unique in that the initial focus is on cybersecurity and it is providing cross training in a number of critical areas as opposed to a single area. In addition, the program has a well-defined education plan and requirements for successful completion. It is designed to develop future cybersecurity professionals that have an understating of Ohio's enterprise and IT security services.

The three cybersecurity apprentices that are currently participating in this new program are just the start for DAS OISP. The plan is to expand this initiative further and make it a permanent source for recruiting cybersecurity resources.

Impact

The Cybersecurity Apprenticeship Program approach will further improve Ohio's overall IT security posture. This type of innovative solution is needed to help ensure that the IT security program continues to grow and mature and that the numerous security safeguards that are already in place for the state are sufficiently maintained. Obtaining these resources is difficult and this solution provides a tangible path to securing cybersecurity staff for Ohio. As a recent Gartner research note indicates, "the unemployment rate for cybersecurity professionals is zero."[3] In addition, Gartner advises that, "the U.S. Bureau of Labor Statistics expects that demand for cybersecurity professionals will increase 53% through 2018."[4] The apprenticeship program allows Ohio to obtain resources within their cost restrictions and deliver value to them in terms of mentorship and training. The cybersecurity apprentices will have exposure to all of Ohio's IT security operations.

The apprenticeship program provides a clear track for career advancement within DAS OISP and through its unique, structured format, it gives the apprentices a hands-on, working knowledge of each IT security area. This helps the apprentice to make more informed decisions about their career and lends itself to greater, long-term job satisfaction.

If these new apprenticeships are successful, it is anticipated that adoption of this model will increase statewide. The State of Ohio envisions this as a recruitment model that will

[3] Olyaei, Sam, Mark Coleman, Matthew T. Stamper. "Adapt Your Traditional Staffing Practices for Cybersecurity," Gartner, 2 May 2018 < https://www.gartner.com/en>.
[4] *Ibid.*

be valuable in other areas of IT as well as in other jobs that may difficult to fill in the current job market.