

State of Oklahoma

2009 NASCIO Recognition Awards Nomination

Oklahoma Cyber Security Group (CSG)

Office of State Finance
Office of Homeland Security
State Bureau of Investigation

Nominating Category:
Information Security and Privacy

Lead, Support, Serve



B. Executive Summary

Oklahoma has over 180 geographically dispersed state entities staffed by nearly 80 thousand people. Disseminating knowledge of and ensuring compliance with the State's security policies and procedures represents a significant challenge. Further, ensuring a coordinated and effective approach to cyber security is hampered by the fact that many state entities lack the requisite expertise and tools.

A statewide Cyber Security Group (CSG) was established during 2004 to help address the situation. This group consists of representatives from every state agency, office, commission and institution of higher education. Each representative assumes a leadership role for their state entity. The goal is the formulation and acquisition of cyber security related knowledge and statewide strategy, such that it facilitates their ability to disseminate and coordinate the same within their respective organizations. As a result, Oklahoma now benefits from a statewide cyber security program.

In 2005, the CSG held their first annual meeting with security briefings, educational workshops and exercises. They began to meet quarterly the following year. These meetings have continued to serve as a primary venue for disseminating knowledge, discussing contemporary cyber security issues and conducting training exercises. Supplementing the quarterly and annual security meetings are the state's cyber security Special Interest Groups (SIGs). The SIG teams are comprised of members from the CSG assembled to address specific areas of need or concern.

Critical synergistic partnerships have been forged across the State's entities and with federal, state and local law enforcement. Supported by a synchronized communications strategy and a formalized education and compliance architecture, this environment promotes comprehensive information assurance initiatives that contribute directly to the prevention of, and detection and response to, cyber crime and other security incidents.

Cross-organization collaboration and buy-in, under the guidance and leadership of the CSG and its SIG teams, has supported the development of statewide policies, procedures and recommendations, sharing of information vital to understanding and preventing security vulnerabilities, and creation of a coordinated statewide incident identification, reporting and management process. Major security education and awareness partnerships have also been developed and fostered across Oklahoma and into the surrounding states.

The leveraging of talent, expertise and resources in this synergistic and collaborative environment has served to make Oklahomans increasingly aware of and better equipped to manage cyber security issues. Moving forward, Oklahoma will enjoy considerable savings and goodwill as security incidents are consistently minimized or avoided altogether, due to its ever-improving security posture.

C. Description of the Business Problem and Solution

Given the substantial number, sizes and geographical dispersion of its state entities, Oklahoma found itself in a disadvantaged position with respect to protecting its information assets. With nearly 80 thousand people staffing over 180 agencies, offices, commissions and institutions of higher education, it was not uncommon to find disjointed and unsuccessful approaches to information security. Even with the best of intentions, many of the state's entities found themselves without the necessary expertise and resources to effectively address or even understand the issues. Further, disseminating knowledge of and ensuring compliance with the state's security policies and procedures in such an environment represented a significant challenge.

Solution

In 2004, Oklahoma sought to bring into line the efforts of its state entities with respect to protecting its mission critical and sensitive information. The result was the formation of a statewide Cyber Security Group (CSG) consisting of representatives from every state agency, office, commission and institution of higher education. Given the goal of formulating and acquiring cyber security related knowledge and a synchronized statewide strategy, each representative was additionally tasked with disseminating and coordinating within their respective organizations.

The CSG began by reviewing statewide standards and recommending improvements, new initiatives and updates to existing policies, procedures and guidelines. To facilitate the dissemination of cyber security information and coordinate the efforts of each state entity, the CSG held its first annual meeting in 2005.

Oklahoma's annual meetings are a full day of security briefings, educational workshops and exercises. For example, the Fourth Annual Oklahoma Cyber Security Seminar (December, 2008) provided an FBI keynote address on Web-based attacks and the insider threat. In addition to a general briefing of Oklahoma's new cyber security initiatives, it featured nine lecture and lab breakout sessions in two instructional tracks. The breakout sessions covered business continuity planning, security threats and corrective actions, data security storage, firewall and defense-in-depth strategies, host hardening, protocol analysis, wireless security, intrusion detection and prevention, and integrating forensics into incident response. The seminar capstone was a cyber incident tabletop exercise (TTX) sponsored by the Department of Homeland Security. The TTX evaluated and enhanced the participants' conceptual and functional knowledge of Oklahoma's cyber incident management procedures. It also featured subject matter experts from the disciplines of public relations, human relations, legal, and forensics investigations, including several members of the FBI Cyber Crime Squad.

What began with the formation of the CSG and an annual meeting has developed into a comprehensive statewide cyber security program. The CSG began meeting quarterly in

2006. These half-day meetings have continued to serve as a primary venue for disseminating knowledge, discussing contemporary cyber security issues and conducting training exercises. Supplementing the quarterly and annual security meetings are the state's cyber security Special Interest Groups (SIGs).

The SIG teams are comprised of members from the CSG assembled to address specific areas of need or concern. They provide guidance on and assistance with establishing project priorities. Historically, SIG teams have led many successful statewide security initiatives; such as providing security awareness training for state employees and developing Business Continuity and Disaster Recovery planning templates for state entities. This effort continues today, with seven new teams formed for 2009.

D. Significance of the Project

The leadership provided by the CSG and SIG teams is facilitating an improved security posture for the State of Oklahoma. Perhaps the most significant contributing factor has been the synergistic partnerships that have been forged across the state's entities and with federal, state and local law enforcement. This environment of teaming has created an open dialog and a critical sharing of information and knowledge.

This dialog is supported by a synchronized communications strategy; including a Cyber Incident Agency Contacts list, a Cyber Security Event Registration system and a Computer Security Incident Reporting application. The contact list facilitates the notification of affected entities whenever a suspected security incident is detected by Oklahoma's Information Security Team; normally when signs of compromised traffic are detected on the state's network backbone. The Cyber Security Event Registration system coordinates the delivery of timely and appropriate security briefings and training events in support of various state security initiatives; including the 2005 rollout of the Oklahoma Computer Crimes Alliance Computer Security Incident Reporting application and Oklahoma's Incident Management Procedures, as well as the statewide Annual Risk Assessments established in 2006.

The statewide Cyber Security Portal was also created in 2006. A repository of security information, it serves to increase awareness and facilitate implementation of the state's information assurance policies, procedures and security templates. The portal disseminates relevant security information and bulletins from recognized security organizations such as the Multi-State Information Sharing and Analysis Center (MS-ISAC).

The CSG partnered with another Oklahoma cyber security initiative in 2007; the Cyber Security Education Consortium (CSEC). Funded by a National Science Foundation Advanced Technologies Education grant, CSEC is led by the University of Tulsa and a

CSG member, the Oklahoma Department of Career and Technology Education. In the face of a significant decrease in Homeland Security funding, the CSG and CSEC partnership allowed the continuation of the CSG annual meetings. This was made possible as CSEC stepped up to play an instrumental role in planning, developing and conducting Oklahoma's Third Annual Cyber Security Seminar with little additional funding.

In 2008, Oklahoma worked to consolidate, leverage and advance its security initiatives with the formation of a comprehensive Information Security Training & Education Program (I-STEP), see Figure 1 on page 6. This program fuses together and builds upon the already established components of cross-organization teaming, synchronized communications, law enforcement partnerships, coordinated incident response, risk identification and mitigation, and information dissemination. The vision is to facilitate an increased conceptual awareness of information assurance issues and objectives while implementing effective planning and management practices to achieve compliance with State and Federal statutes. In short, I-STEP seeks to leverage and develop existing education and administration programs to ensure compliance with defined policies, procedures, standards and guidelines through effective governance and accountability.

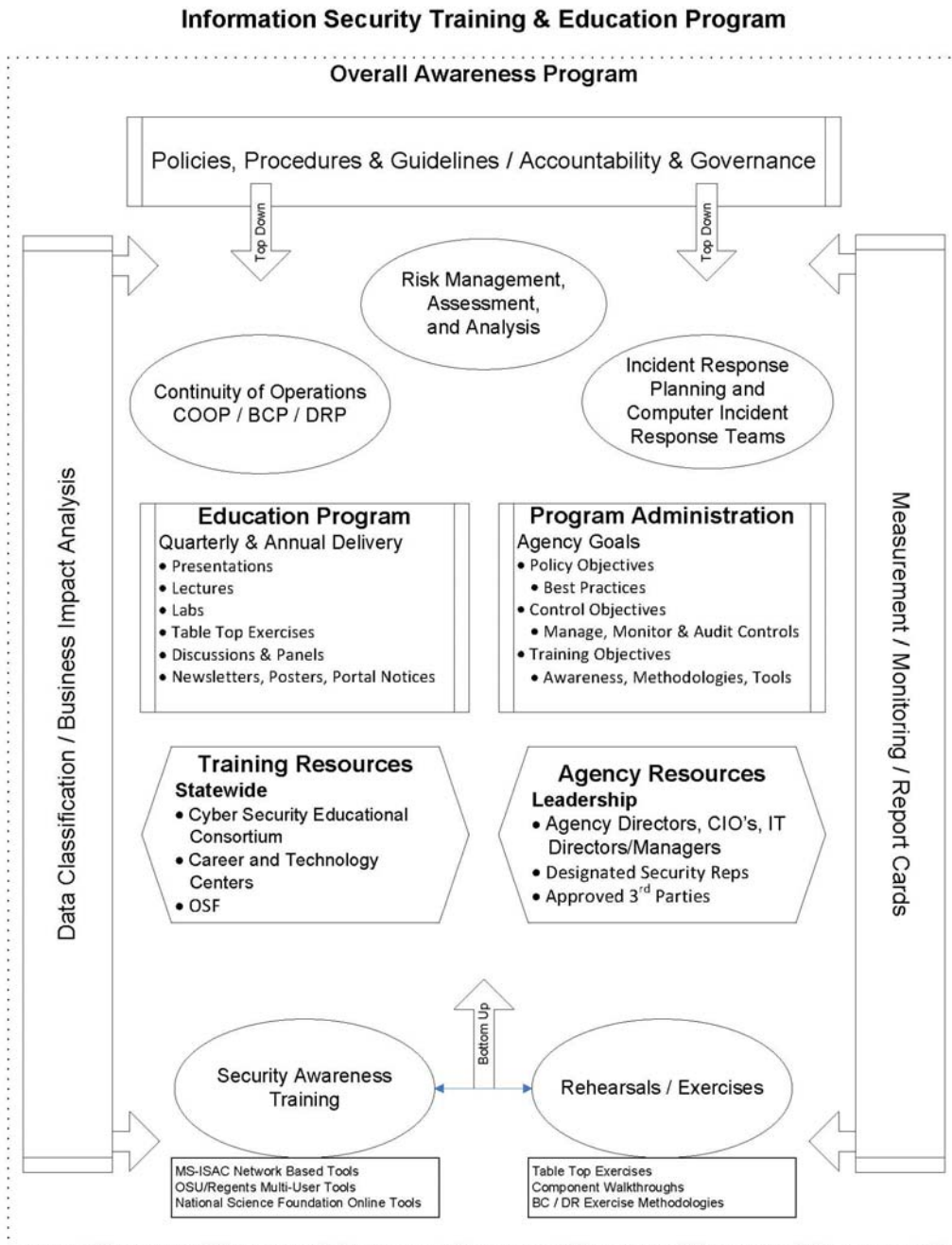
Central to the I-STEP strategy are education and program administration. The I-STEP Education Program seeks to leverage and supplement the existing quarterly and annual meeting format with real-time delivery mechanisms. The goal is to provide presentations, lectures, labs, exercises, online training, courses and materials to raise security awareness and address the state's top vulnerabilities as identified by the annual risk assessments. The plan is to research and utilize existing free or low cost online education programs such as MS-ISAC and ACT Online, while continuing to work with the Oklahoma Department of Career and Technology Education and CSEC to develop additional training materials and venues.

Program administration is structured to address the security goals for each of Oklahoma's entities. These include objectives of policy, training and control. Policy deals with establishing best practices for meeting the state's information assurance goals. Training takes into account not only security awareness but also methodologies and tools. Control embraces the idea of managing, monitoring and auditing the security environment. The plan here is to further engage the directors and managers of Oklahoma's entities, as well as approved third parties, to help lead this effort.

I-STEP embraces five focal areas; including security awareness training; risk management, assessment and analysis; continuity of operations; incident response planning and computer incident response teams; and rehearsals and exercises. The key inputs to I-STEP are data classification and business impact analysis, while the key outputs are measurements (baselines), monitoring (exception reporting) and report

cards (gap identification). The 2009 SIG teams were established with these targets in mind.

Figure 1



E. Benefit of the Project

Cross-organization collaboration and buy-in, under the leadership and guidance of the CSG and its SIG teams, has created an environment that contributes directly to the prevention of, and detection and response to, cyber crime and other security incidents.

The CSG has provided the architecture for effectively protecting the state's information assets by supporting the development of statewide policies, procedures and recommendations and facilitating the timely and appropriate sharing of information vital to understanding and preventing security vulnerabilities. Risk is minimized as the coordinated efforts of the CSG and its SIG teams lead to the design and implementation of effective countermeasures against threats and threat agents wishing to abuse or damage those assets.

Partnerships with law enforcement and educational institutions has led to further synergies; with the former contributing to a coordinated and timely containment of security breaches and preventative actions, and the latter leading to expanded education opportunities both in Oklahoma and the surrounding States.

The Cyber Security Education Consortium has fostered security education programs in Arkansas, Colorado, Kansas, Louisiana, Tennessee and Texas. The CSG and CSEC partnership is leveraging these relationships to help promote Oklahoma's security education and awareness efforts. For example, the Fourth Annual Oklahoma Cyber Security Seminar featured speakers not only from Oklahoma institutions, but also CSEC instructors from Colorado, Louisiana, Tennessee and Texas. In return, Oklahoma has offered to help model the event in their states.

The threats we face as a state and nation are real. Fraud and intellectual property theft resulting from the loss or compromise of sensitive data, and the criminal exploitation of children are but a few examples of what is at stake.

In short, Homeland Security and other monies have been used to provide effective and far-reaching cyber security educational initiatives through the leveraging of talent, expertise and resources in this synergistic and collaborative environment. As a result, Oklahomans are increasingly aware of and better equipped to manage cyber security issues. Moving forward, Oklahoma will enjoy considerable savings and goodwill as security incidents are consistently minimized or avoided altogether due to its ever-improving security posture.