

State of Oklahoma

2009 NASCIO Recognition Awards Nomination

Oklahoma Computer Crimes Alliance

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

**Nominating Category:
Cross-Boundary Collaboration
and Partnerships**

Lead, Support, Serve



B. Executive Summary

Oklahoma introduced federated standards by implementing statewide information security policies, procedures and guidelines to establish statewide best practices. The need to enforce these standards led to the formation of a statewide cyber security coalition. This group subsequently identified the absence of centralized incident reporting and management as both a threat and a vulnerability to operational integrity.

The security coalition consists of three state entities, including one hosting agency and two statewide law enforcement agencies. The Oklahoma Office of State Finance (OSF) has responsibility for establishing statewide policies, procedures and guidelines; the Oklahoma Office of Homeland Security (OKOHS) is closely aligned with the Department of Public Safety; and the Oklahoma State Bureau of Investigation (OSBI) focuses on intrastate law enforcement.

Providing a solution to address computer related incident reporting and management involved establishing a process for all state entities to work with law enforcement, if criminal activity was suspected. OSF, OKOHS and OSBI worked with the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (USSS) to establish a cooperative relationship. The FBI and Secret Service had already established relationships with local law enforcement.

An alliance between the FBI, Secret Service, OSF, OKOHS and OSBI established the primary parties responsible for ensuring that computer related incidents were reported, tracked and managed statewide. The Oklahoma Computer Crimes Alliance (OCCA) was created, which included representation from 20 Federal, State and Local law enforcement offices. OSF is the central point of coordination for collecting and reporting computer related incidents statewide.

OSF and the OCCA defined system requirements and procedures needed to report, track and manage computer incidents statewide, which the State's portal vendor, NIC, used to develop an automated system. OSF updated the statewide information security policy to include mandatory procedures for computer related incident reporting with instructions explaining how to use the automated system. OSF monitors state networks for malicious activities that could otherwise go undetected.

Monitoring activities coupled with the incident reporting system have identified numerous cyber security threats and alerted state entities involved. The OCCA reviews incidents to determine if further investigation is warranted. Since September 11, 2006, 27 incidents were logged in 2006, 56 in 2007, 17 in 2008, and 9 (so far) in 2009. This solution has enabled the identification and removal of malware, identified multiple offenders not adhering to statutory regulations on obscene material, and it has enabled law enforcement to identify and prosecute suspected cyber security offenders.

C. Description of the Business Problem and Solution

Problem Statement

The State of Oklahoma needed a solution to: facilitate computer related incident reporting, tracking and management; identify security threats and improve security awareness with all state entities; and cooperate with the appropriate Federal, State and Local Law Enforcement Offices in the classification and investigation of computer related incidents.

Barriers and Challenges

1. Establish central points of contact within Federal, State and Local law enforcement offices.
2. Establish a statewide single point of contact for reporting and classifying all computer related incidents.
3. Establish a statewide network of security contacts responsible for incident awareness and reporting.
4. Establish a proactive threat monitoring solution to assist state entities in the identification, reporting and management of computer related incidents.
5. Establish procedures for reporting and managing incidents.
6. Establish a methodology and an automated system for reporting and managing computer related incidents.

Assessment and Decision Making Process

The combined solution has been fully operational for 2 years and 9 months since it went online on September 11, 2006.

Solution

This project involved Federal, State, Local and Private sector resources, whose combined efforts produced custom cyber security controls for the State of Oklahoma. The FBI championed the project on behalf of law enforcement and they funded the hardware (servers and related network components) to ensure the integrity and confidentiality of the information collected and retained by law enforcement. OKOHS funded the purchase of network monitoring tools and provided a secure operating environment for the law enforcement components of the solution at the Department of Public Safety. NIC, a private sector third party responsible for the development and maintenance of Oklahoma's State portal, provided the programming resources to develop the incident reporting and management application software. OSF provided the resources for project management, system requirements specification, development of mandatory incident reporting procedures and the identification and coordination of cyber

security representatives from all state entities. OSF also developed the system documentation and provided training and support for use of the automated system.

Once an agreement was reached to form the OCCA, the security coalition completed requirements for the automated system and the procedures needed to report, track and manage computer incidents statewide. NIC used open source tools (PHP, MySQL, and Apache) to develop the application software. After development was complete, OSF worked with NIC to test and accredit the automated system. OSF updated the statewide information security policy to add mandatory procedures for computer related incident reporting, including instructions explaining how to use the automated system.

OKOHS provided Homeland Security grant funds to OSF for the acquisition of network monitoring tools to facilitate proactive identification and elimination of cyber security threats. These tools improve security by lowering the risk of state assets being exposed to malware and reducing the risk of data loss. OSF uses these tools to monitor the state network for malicious and illicit activities that could otherwise go unnoticed. Using a combination of these tools and the statewide incident reporting system, Oklahoma has identified numerous cyber security threats, notified the state entities involved and reported incidents to the OCCA. After the incidents have been confirmed, OCCA evaluates the incident to determine if further investigation is warranted.

D. Significance of the Project

The implementation of this solution has improved statewide security by:

1. Increasing the awareness of computer related issues;
2. Providing an automated solution to report, track and manage computer related incidents;
3. Providing tools to monitor the state network and identify cyber security threats;
4. Providing law enforcement with valuable information and insight into security incidents throughout the state, as well as a secure environment to manage incident details that can be used as evidence to prosecute suspected offenders; and
5. Providing state entities with an automated notification and alert system.

Previously, the state had no method of collecting metrics on computer related incidents or threats. Each state entity now has a designated primary and secondary cyber security representative with secure access to the statewide incident management system. In addition to providing incident reporting and tracking capabilities, the system also includes: an automated statewide cyber security alert notification feature; a cyber

notes section with updates on recent threat activities; hyperlinks to national cyber security technical alerts, bulletins, tips and blogs; and system administrative capabilities with secure controls for law enforcement use only.

The availability of the system was officially announced at the State's second annual Cyber Security Seminar in 2006, at which time training was provided to all in attendance. This training was followed up with a statewide email announcement that included copies of the mandatory incident reporting procedures, with documentation on how to use the automated system and how to contact OSF's Helpdesk to get support for the solution.

OSF, OKOHS and OSBI formed a triumvirate to ensure that State statutes and statewide policies, procedures and guidelines are followed. OSF reports questionable activities it identifies to the state entity or entities involved, giving them an opportunity to initially investigate and formally report their findings. If the entity is unable to respond or report, OSF provides assistance as needed, including reporting on their behalf. The triumvirate has the authority to intervene and act on behalf of the entity, if the threat is considered serious enough to put others at risk.

All state entities are required by policy to have an externally facing firewall at the perimeter of their internal network. OSF uses anomaly detection tools to monitor the traffic entering and leaving these firewalls for abnormal traffic patterns and for known types of traffic that indicate the presence of aberrant conditions. An additional feature of the monitoring tools is the ability to place a probe within a state entity's local area network and identify the host or hosts that have been compromised.

E. Benefit of the Project

This project was undertaken to enhance security by providing the improved controls needed to safeguard state government assets. Prior to implementing this solution, computer related incident reporting was inconsistent and uncoordinated at best. Following the implementation of this solution, state entities now follow established computer related incident reporting procedures using a centralized system that automatically submits incidents to the Oklahoma Computer Crimes Alliance for evaluation and investigation as needed.

With the implementation of statewide monitoring tools, OSF can now identify malicious and illicit activities by examining network traffic for anomalous behavior that indicates the presence of suspicious activity. This capability enables OSF to inform State entities when it appears their internal networks have been compromised. These tools provide reports that let us know if someone violates State statutes or policy by using inappropriate software or by connecting to malicious or inappropriate Internet locations.

The use of this solution has afforded Federal, State and Local law enforcement offices the opportunity to conduct local investigations, identify and prosecute offenders and to collect valuable intelligence information that has improved the quality and quantity of incident reports on state and national levels. Since this solution was implemented, Oklahoma has identified, eliminated and/or prevented the spread of malware (viruses, Trojans and Botnets) within numerous state entities.

Another consequence of this solution is the formation of a Cyber Security Focus group consisting of volunteers from the community of statewide cyber security representatives. The purpose of this group is to review statewide standards and recommend improvements, new initiatives and updates to existing policies, procedures and guidelines. This group has been instrumental in providing guidance and assistance in establishing project priorities and the development of templates (i.e., Business Continuity and Disaster Recovery) for use statewide.

On multiple occasions, state entities that were unaware of any threat to their environment were notified they had traffic within their internal network exhibiting patterns of behavior consistent with compromised host activity. The OCCA provided assistance to help them determine the level of vulnerability and exploitation that had occurred. In some cases, the information collected also contributed to the identification and subsequent removal of external threat sources by law enforcement. Prior to implementing this solution, such cases might have spread beyond the initial entity impacting others within the State.

This solution has improved the security posture of State government by providing a solution that:

1. Identifies and reduces automated and directed external threats;
2. Reduces operational vulnerability by providing an automated system to report, track and manage computer related incidents;
3. Establishes and maintains a statewide network of cyber security representatives, which increases each participants awareness of security issues;
4. Establishes state-level leadership in the form of the security coalition that acts as a triumvirate to ensure State statutes and statewide policies, procedures and guidelines are followed; and
5. Establishes a Cyber Security Focus group consisting of members from the overall community of cyber security representatives, who meet regularly to review statewide standards and recommend improvements, new initiatives and updates to existing policies procedures and guidelines.