# SOUTH DAKOTA

## ENTERPRISE CYBER SECURITY OPERATIONS


**Jim Edman**
**Deputy Commissioner**

bureau of information & telecommunications

**(605) 773-4165**
**Jim.Edman@State.sd.us**

INITIATION DATE: NOVEMBER 2012 | COMPLETION DATE: DECEMBER 2013

## Executive Summary

State CIOs, guardians of state data/technology resources, are too familiar with the threats that haunt us all and are rightfully concerned their security services may be insufficient to prevent them from being the next victim of a security breach. Cyber security is currently complicated and evolving rapidly. The mitigation of risks aggregated across a large enterprise requires extensive cooperation and expertise. Securing the authority and responsibility to apply best practice security measures and solutions is difficult. A confederation of independent I/T teams of varying size and mixed skillsets responsible for the management and delivery of services across individual departments and various branches and levels of government faces significant political, technical, and staffing hurdles when challenged to implement enterprise security procedures, policies, and practices.

As reported in NASCIO's Top Ten Priority survey, Cyber Security and Consolidation/Optimization have been recognized by state CIOs as priority concerns for each of the past ten years. South Dakota's experience suggests implementation of Enterprise Security is eased when Consolidation/Optimization efforts are well underway. South Dakota had successfully consolidated I/T services over a period of 18 years. In late 2012 South Dakota leveraged this experience to embark on a program to address enterprise-wide security issues in a cost efficient manner through a single technology organization with trained cyber security professionals armed with the necessary authority, resources, and tools. Through this project, South Dakota has assigned and developed staff, defined policies and practices, and acquired necessary resources and tools to organize a consolidated cyber security solution. This complete enterprise-wide framework assigns strategic and tactical responsibilities for cyber security services supporting South Dakota's Executive, Legislative, and Judicial branches, Constitutional offices, and K12 public schools.

> This solution addresses workstation hardware and software, wired and wireless networks, Internet access, internal and external-facing server systems, internal and outsourced development of business software. Strategic and policy responsibilities incorporated include planning, monitoring, auditing, compliance, disaster recovery, business continuity, and education/awareness partnerships.

The overarching goal was, and remains, to reduce statewide risks and improve defense systems. This approach has improved visibility of cyber security among clients, focused efforts on a single enterprise plan, established layers of expertise across multiple platforms, eliminated redundant responsibilities, and most importantly, improved cyber defense systems.

## Business Problem and Solution Description

State governments face constant pressure to offer more services in more methods while holding level or reducing government expenses. A byproduct of this increasing dependence on technology is the heightened importance of cyber security. As national, international and state-sponsored cyber criminals target state systems our defense often remains disjointed and incomplete. Disputes over jurisdictional boundaries increase personnel costs and hamper efforts to implement cohesive solutions. Despite a shared common goal to protect technology resources a combination of lack of expertise, organizational challenges, and disagreements concerning which of a myriad of technology solutions to implement lead to inefficient, disparate, isolated, and questionable solutions.

South Dakota offers a complete cyber security solution to state government and the K12 community; protecting the personally identifiable information of constituents, health records, business data, statewide K12 student information system, and other data highly attractive to cyber criminals, the breadth and scope of the implemented framework distinguishes the South Dakota project from others. Holding secure client desktops, the networks they share, the business applications and web services, and integrated with governing policies and procedures, this cohesive assignment of enterprise-wide strategic and tactical responsibility provides South Dakota with the ability to efficiently and effectively defend I/T resources.

- The human element is the most important aspect of the project.

Representatives of the Desktop, Network, Enterprise Systems and Software Development teams comprise the Security Operations Team (SOT) and daily review the previous day's empirical data collected by diverse security and logging systems.

The discussions review specific and corroborating evidence, searching for known attack vectors. The team has been assigned enterprise authority to coordinate efforts in strategy, detection, analysis and operational management. Including representatives from all technology teams creates powerful synergy to quickly solve problems.

- As an example of the process employed by the SOT, a review of log data from all web servers may begin by passing log data through the BIT Security Incident and Event Management system to search for common attack vectors. The logs may also be processed by custom built parsers to identify reconnaissance attempts, brute force attacks and other classes of attack methods. Endpoint software provides alerts for network and malware breaches, while two separate and independent network IDS/IPS and antivirus systems scan for incidents in transit. Six different categories of technology encompassing thousands of devices are fed into a single management system. Aggregation of logs with automatic, smart threat review is critical to any analysis of security data. The over 8,000 security events collected every second are categorized by severity each morning. Following a risk analysis of this distillation an average of 20 incidents per day are selected for further

investigation. Logs for these incidents are forwarded to the MS-ISAC for third-party verification. MS-ISAC incident notification is excellent but rarely does the MS-ISAC notify South Dakota of an event that the State is not already in the process of addressing.

■ Multiple client protection layers exist to protect against malware threats. Intrusion detection, prevention, software scans and policies defend against virus, worms, trojans, and spyware threats. Security rules and heuristics identify and rate accessed files to protect against new, sophisticated, unknown and mutating threats that evade traditional security measures. Protection is accorded to 9,400 state government machines and 84,000 K12 computers, while active management of endpoint protection gathers event information for immediate analysis. Issues can be delegated to technologists for action regardless of location or school. For example, protection from the April 2014 Microsoft Internet Explorer zero-day vulnerability was provided via a statewide definition update deployed the day of the vulnerability disclosure; the Microsoft patch was deployed and verified the next business day.

■ An improved process to deploy and confirm installation of software patches and upgrades demonstrates additional security achieved through the project. Multiple tools cross-check and confirm installation success or failure. Implemented standards for computer hardware and utilization of a uniform software clone facilitate employment of security best practices to increase the probability the patch/upgrade will be successfully installed. In 2013, 374 patches for nine standard software products were expeditiously and successfully deployed and installed statewide.

■ A single, statewide directory provides Identity and Access Management on an enterprise-wide basis. Application authentication and access is controlled through single sign-on without the need of disparate authentication systems. Utilization of a single system and its accompanying single log stack enhances security while reducing complexity. Resource access is controlled via regularly reviewed group policies. Minimum needs determine access and effectively preclude the assignment of administrative privileges.

■ Unified wireless network services use 802.1x authentication and are compliant with the Advanced Encryption Standard. Policy management and platform control provides secure wireless access, ensuring user and device identification.

■ Consolidation of diverse mail systems facilitates email security. Incoming and outgoing messages for 94,000 government and K12 accounts are filtered and scanned by independent perimeter processes providing a unified threat management solution through ‘deep content inspection’. Email encryption solutions protect sensitive data (financial, PII, medical) while in transit and prevent delivery of any unencrypted messages meeting “confidential” criteria.

■ Remote/mobile access is important for many clientele. A statewide mobile device management solution provides safe access across multiple platforms through both policy and technical solutions. State-owned devices are permitted protected access to enterprise wireless network, while third-party solutions provide “bring-your-own-device” services and protection.

■ South Dakota has established stringent standards and processes to govern the construction, verification, and deployment of internal and contracted software development.


Vendor-provided and in-house applications endure design and operational reviews before graduating to User Acceptance Test (UAT) and Production status. Governance mandates lifecycle training for each developer and analyst; adherence to standards is encouraged through regular policy and compliance reviews of development projects. Construction dictates requirements and data gathered evolve from and support business functionality. Verification validates design and construction against enterprise security requirements. Contracted development projects must pass the same scrutiny as in-house projects. In one instance a vendor-developed application required 34 security evaluations spanning four months before graduating to the UAT environment. Deployment includes regularly scheduled evaluation of existing systems against constantly changing attack vectors.

■ Geolocation management of source IP addressing limits website accessibility. New enforcement rules restrict which countries can access specific departmental web sites, allowing the State to block certain geographic locations based on attack analysis or by utilizing research identifying known suspicious networks.

■ The enterprise database represents the ultimate "vault" of data and requires conclusive protection. New database protection measures were implemented throughout 2013. New encryption standards for PII data, independent SQL injection protection, stringent complex password requirements and encrypted data in transit add safeguards to an appealing environment under constant attack.

■ Security requirements are incorporated into procurement documents during the proposal stage and included in project contract terms.

Including criteria for standards for design, evaluation, testing and hosting services early in the project ensures vendors understand expectations prior to submitting a proposal.

■ Security programs are founded on policies and procedures defining acceptable behaviors and guidelines while promoting positive practices. Regulators have established high expectations regarding configurations and policy definition. Audits, compliance activities and policy development/refinement are now coordinated through a single group directed by the CSO ensuring enterprise-wide conformity while avoiding duplication of efforts. This compact administrative structure allows NIST-based policies, risk assessment lessons, and procedures and practices implemented to address audit findings in one department to quickly be implemented across all agencies to maintain a uniform enterprise security posture.

■ In the Rushmore State, as in other states, cyber security education and training for employees presents a monumental challenge. The human firewall is as critical as its technical counterpart. To improve employee awareness of their role in cyber security an enterprise-wide online class was developed and distributed, completion is monitored and new modules are released and delivered regularly. Additional education content is delivered through a directory-enforced Internet browser splash screen. Recent usage examples include increasing employee awareness of the Target breach, the termination of Windows XP support by Microsoft and the Heartbleed vulnerability; all encouraging employees to incorporate cyber security practices in personal home environments.

■ Partnerships remain an essential aspect of the State's effort. Our Security Information Council was formed to share operational experiences and challenges across political governmental boundaries.

Chaired by the state Chief Security Officer and with representation from the different branches of state government, higher education, K12 and local governments, the Council biweekly reviews cyber security projects, concerns and issues that extend beyond the traditional state enterprise.

## Significance of the Project

■ Security is not a project to be finalized and reported as complete; rather it is a constant struggle between the nefarious and the entrusted. The project's greatest significance is measured by the substantial reduction of risk to state information systems and data. While reduced costs and greater productivity in our programs and services are clear successes, decreased risk and threat exposure for our customers and all South Dakota citizens is the principle success. This risk reduction can be directly attributed to the assignment of enterprise strategic and tactical responsibilities to a single program. Cyber security has many components, a weakness in any component can quickly be translated into an exposed vulnerability. Employing a uniform approach has permitted the State to integrate a total security framework across state government and K12 communities.

■ The State security lifecycle aligns government and K12 needs through efficiencies in staffing. The approach embraces "business by business experts" and "technology by technologists". This centralization builds a deep knowledge base in defined areas of expertise. The segregation of technologists, specifically cyber security staff, allows the State to develop employees whose skills are shared across platforms and across agencies. Individual technologists collaborating on enterprise solutions are empowered to quickly address operational issues that may span traditional organizational boundaries. Patches are delivered, policies updated, best practices applied, and education delivered at the speed of business.

## Benefits of the Project

The benefits of the consolidated enterprise-wide program implemented in South Dakota – across twenty two executive branch agencies, the legislative and judicial branches of state government, six constitutional offices, and 151 public school districts – significantly outweigh those that can be attributed to a confederation of cyber security programs of varying size and with mixed skillsets. Disjointed distributed teams struggle to find qualified staff, especially in a state that epitomizes the characteristic of “profoundly rural”. The decision to pursue cyber security by assigning responsibility to a consolidated enterprise program has eliminated cross boundary jurisdictional disputes and provides an aggressive uniform security posture to protect state technology resources.

The South Dakota cyber security program reduces costs by sharing core services across government offices and K12 schools. A central security team of ten full time employees, a personnel services expense of approximately $750,000, is assigned authority for the core of the security program. Security team members are embedded within the networking, enterprise systems, desktop support, and development teams. Oversight authority for this agile, focused and well-trained team is assigned to the Chief Security Officer. If only half of the departments and schools had elected to invest in professional staff to support individual services, rather than opting for a centralized security organization, staffing costs would have easily passed seven million dollars. Instead, organizing a small group of experts exponentially increases efficiencies while saving citizens over six million dollars annually. Centralized procurement results in savings and cost-avoidance. Statewide firewall purchases were less than $325,000 for 151 school districts and state government. Providing employees an online security awareness educational program, incorporating security concerns early in the process of procuring applications or services, and collaborating with agencies for compliance audits has increased the number of end-user security questions and concerns raised by state employees. Similar levels of success reach into other security sub-disciplines, further demonstrating the effectiveness of our program’s design. A reduced number of firewalls and related hardware platforms, consistent training and education, and mature software development standards exist as important areas where efforts are not duplicated.

While financial investments have been necessary to build a talented, focused, enterprise security team and provide the resources, training, and tools necessary to address assigned responsibilities, the notable investment is the executive decision to remove jurisdictional boundaries and to address cyber protection as a necessary enterprise service and the commitment of staff to define and implement innovative, complex solutions to provide this service. All of these efforts support Governor Daugaard’s stated goals of having our constituents online rather than in line. Cyber security remains paramount in maintaining public trust.