COLORADO
Governor's Office of
Information Technology
Serving people serving Colorado

Secure Colorado: Achieving Quick and Sustainable Risk Reduction

Nomination Category	Cybersecurity
Nomination Contact	Tauna Lockhart 303.764.7731 tauna.lockhart@state.co.us
Project Initiation Date	July 1, 2013
Project Completion Date	November 30, 2014

I. EXECUTIVE SUMMARY

The often named “Year of the Data Breach” -- 2014 -- proved to us that no enterprise, regardless of the size of security investment, is immune to attack. Attackers’ weapons are changing daily, technology is advancing exponentially, and businesses are evolving constantly -- requiring rapid response and preventative tools to detect and thwart the increasingly sophisticated level of cyber attacks.

With both the public and private sectors facing increasing threat to their IT landscape that makes their information and technology assets vulnerable to attackers, state government is uniquely targeted because of the amount of sensitive and valuable data on state systems. At the Colorado Governor’s Office of Information Technology (OIT), our security team averts approximately 800,000 malicious events each day. As the increased volume and level of sophistication of security threats continues to grow, we recognized a new approach was needed for protecting State of Colorado information and assets.

That new approach came through Secure Colorado, the state’s first cybersecurity strategic plan. It is focused on achieving quick and sustainable risk reduction at a reasonable cost, while promoting an environment of technology innovation, adoption of open source and cloud based technology and the open sharing of data where appropriate. Secure Colorado is a huge innovation in cybersecurity for the government sector, and it has revamped the state’s approach to security by aligning priorities and control framework.

II. BUSINESS PROBLEM AND SOLUTION DESCRIPTION

The Colorado Information Security Program was created through legislation in 2006, and although Colorado was one of the first states to pass such legislation, the program was constrained by the lack of a consistent and cohesive strategy aligning the state’s mission to cost-effectively deliver value-added services to Coloradans. In addition, the threat to Colorado systems and data had been evolving and growing at a staggering pace. During the economic downturn, state government spending was limited and required Colorado to look for unique and novel approaches for affordably driving down risk.

With those conditions in mind, Colorado’s Chief Information Security Officer (CISO), in cooperation with other members of OIT’s executive leadership team, created a plan for a cost-effective cybersecurity strategy.

Here are the actions taken in late 2012 by the State of Colorado:

1. Stopped the purchase and renewal of all new security tools and products
2. Performed a gap analysis evaluating the effectiveness and cost of existing

controls against the threats currently faced by the state

3. Evaluated the structure, organization, and funding of the Colorado Information Security Program
4. Put together an advisory board of state and national cybersecurity experts to assist the CISO's security team in developing a cybersecurity strategy

Based on this work, the CISO and executive team created Secure Colorado -- the state's first cybersecurity strategic plan, which went into effect on July 1, 2013. This strategic initiative involved revamping the state's approach to security by aligning our priorities and control framework with the Top 20 Critical Security Controls for Effective Cyber Defense (The SANS Institute), starting with the sub-controls referred to as "the first five." These controls were selected because they could be quickly and affordably implemented, some with open source tools, and have been proven to dramatically decrease an organization's risk of compromise. In fact, highly regarded research has shown that when an organization successfully implements the first five critical controls it can quickly and cost-effectively reduce risk to its information technology assets by as much as 85-90 percent.

Each of the 20 Critical Security Controls includes multiple sub-controls: 182 total sub-controls, with 75 "quick wins." The quick wins for each of the 20 controls were prioritized for implementation for this project. OIT expects to continue to mature these controls by prioritizing the implementation of additional sub-controls based upon risks and threats, evolving technology and business strategy, cost, and other factors.

The implementation approach was designed so that local governments, many with very limited resources, could achieve similar results at a price point they could afford. OIT's use and selection of tools were intended to achieve the maximum amount of integration, reporting, and extensibility.

III. SIGNIFICANCE

In March 2015, The Brookings Institution cited Colorado as one of only two states to have demonstrated a "solid and robust" understanding of the importance of integrating cybersecurity in their strategic IT plans, and Secure Colorado is the reason for this innovation in applying cybersecurity's importance.

Across all industries, data breaches and the protection of business-critical data remain a top concern. While the government sector has remained committed to making investments to prevent data breaches -- implementing rigid security best practices, undergoing comprehensive product testing, developing compliance regulations, etc. -- government agencies continue to experience breaches. Since the threat landscape continues to grow, it is critical that security dollars are spent to maximize risk reduction while not impairing innovation and business growth.

Colorado was the first state in the nation to implement the first five sub-controls of the Top 20 Critical Security Controls. OIT's security program has made *organizational changes* and *partnerships* that will significantly reduce the overall risk to the state and demonstrates value to the residents of Colorado. These relatively simple changes are repeatable, sharable, and cost effective -- and could easily be adopted by other governmental entities.

Organizational, Procedural and Technical Changes

- Alignment of the team to proactively address security and manage risk. By organizing the teams according to their strengths and interests, there has been a more efficient use of resources and, most importantly, a solid structure to proactively address security, manage risks, and to apply this consistently across the state.
- Establishment of a risk and audit committee to ensure that risk assessments are being performed, and that risks are being tracked and reduced, in a consistent manner across all agencies.
- Remediation of audit findings and known vulnerabilities. Audit findings had been piling up for a number of years, and a project was established to remediate these audit findings and operationalize the ongoing remediation of vulnerabilities and findings -- whether self-discovered or audit-related. There have even been auditing entities (such as the IRS) commending Colorado on the improvements they've seen, and the resulting increase in comfort they have over the environment.
- Implementation of the "first five" critical security controls resulting in an inventory of connected devices and deployed software, as well as an estimated 75 percent reduction in malware events
- Establishment of metrics to provide transparent measurement into the program.
- Replacing outdated technology with transformative next generation technology. For example, we implemented next generation firewall technology for better filtering for individual agency needs and to provide increased visibility and automated prevention for advanced threats.
- Creation of a SECURE system development life cycle (S-SDLC) for application code reviews at appropriate times in the implementation and change process.
- Establishment of a budget dedicated to Cybersecurity Improvements, with the goal of improving this budget, over time, to equate to 5 percent of the annual IT spend.
- Increased testing of cyber attack preparedness and response. OIT completed a combined exercise with members of the steering committee and Regis University to practice response to cyber event (August 2014). OIT is currently planning a combined cyber exercise with the Colorado National Guard to test response procedures (July 2015).
- Configuration of secure standards. The state has adopted the benchmark standards and guidelines as produced by the Center for Internet Security (CIS) and partnered with CIS to ensure all new systems being built are properly

hardened and assessed prior to going into production. As owner of this initiative, the CISO's security team has trained all system, network, and desktop support staff across the enterprise to use the CIS hardening guides available on the Internet to configure existing systems. In addition, through contracts and purchase agreements, OIT now requires all vendors to provide new systems already configured according to CIS hardening guidelines. To verify compliance with this initiative, the OIT security team audits all state systems against the CIS benchmarks on a monthly basis.

- Reduction of users with administrative privileges. Using group policies within Active Directory, the CISO's security team significantly reduced users with administrative privileges throughout the enterprise.

Partnerships

The Secure Colorado partnerships formed help to share threat intelligence information, research and development efforts and best practices.These partnerships are utilized to promote discussions and cooperative engagements that will enhance cybersecurity for all Colorado residents. Lastly, these partnerships are instrumental in testing and improving our response to cyber events.

- The Cybersecurity Steering Committee is a monthly working group for information sharing. Participants include OIT, Colorado National Guard, Department of Public Safety, Colorado Division of Homeland Security and Emergency Management, Colorado Bureau of Investigation (CBI), FBI, Secret Service and others,
- The Cybersecurity Task Force was established through legislation and is comprised of OIT Office of Information Security, CBI and Colorado Division of Homeland Security and Emergency Management. This team is led by the FBI and is responsible for discovering, investigating and prosecuting instances of cyber crime targeted against Colorado

IV. BENEFIT OF THE PROJECT

As a result of Secure Colorado, the State of Colorado has achieved the following measurable improvements:

- More than 95 percent of known servers and more than 95 percent of known computing devices (desktops, laptops) are now being managed by our security team.
- A 16 percent increase in the number of state systems under near real time monitoring and management by the security team at OIT over FY2013. As of FY2014 more than 95 percent of all state systems are being monitored, audited and managed in near real time.

- More than 90 percent of managed systems are being audited for CIS hardening compliance.
- More than 75 percent reduction in the average number of monthly malware infections, with no major infections since December 2012.
- Approximately $833,000 in cost avoidance and savings through the elimination of redundant and non-effective security tools. These savings were re-purposed to implement the first five controls.

As a progressive and innovative state, our security team continues to evolve and embrace new technologies, and Secure Colorado will evolve as well. Coloradans are demanding mobile applications, social media interaction and other new ways of interacting with state government -- and the State of Colorado has to include security in these innovations from the very beginning in order to stay ahead of attacks.