Colorado's Strategy for Information Security and Risk Management

Fiscal Years 2014 - 2016

Secure Colorado

Governor's Office of Information Technology

June 1, 2013

Table of Contents

Section I – Introduction and Background

A Call to Action

The need to manage cyber security is an increasingly strategic tenant of any mature enterprise. In addition, to be successful, security must incorporate the right mix of technology, people, and processes and properly balance risk against the overarching need to accomplish the State's mission of providing efficient, elegant, and effective services to Coloradans.

Although we are not alone in our need to protect ourselves, governments are uniquely being targeted. In fact, the State of Colorado's networks, systems, employees, and endpoints are continuously under attack. As of December 2012, state systems are being hit by approximately 600,000 malicious events per day. In addition, our enemies' attacks are becoming more sophisticated, persistent, and targeted. In the last six months, the State has been hit by advanced persistent threats and malware that was highly customized and targeted to avoid the State's defenses and create maximum damage.

While the volume and sophistication of attacks are increasing, the most recent economic downturn has had a serious, detrimental impact on cyber security protective resources and measures deployed throughout state government.

The time has come to take action in order to proactively and preemptively protect the residents of Colorado!

This strategic plan, known as **Secure Colorado**, is a three-year initiative focused on making strategic decisions and investments to protect the data Coloradans have entrusted to state government. **Secure Colorado** outlines the strategic goals and initiatives of the Colorado Information Security Program to safeguard the State's information assets and assure the confidentiality, integrity, and availability of the information vital to achieve the State of Colorado's mission.

Respectfully,

Jonathan C. Trull

Jonathan C. Trull
Chief Information Security Officer

600,000

Number of cyber attacks launched against the state each day

680%

Increase in significant cyber security threats against U.S. government systems 2006 – 2011

94 Million

Number of Americans' files in which personal information has been exposed to potential identity theft through data breaches at government agencies since 2009

Information Security Governance

The Colorado Information Security Program was created through legislation in 2006. According to Colorado law (Part 4 of Section 24, Article 37.5 of the Colorado Revised Statutes), the Colorado Information Security Program is overseen by the Chief Information Security Officer (CISO) and applies to "public agencies." A public agency is defined as:

> ...every state office, whether executive or judicial, and all its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

According to statute, the CISO shall:

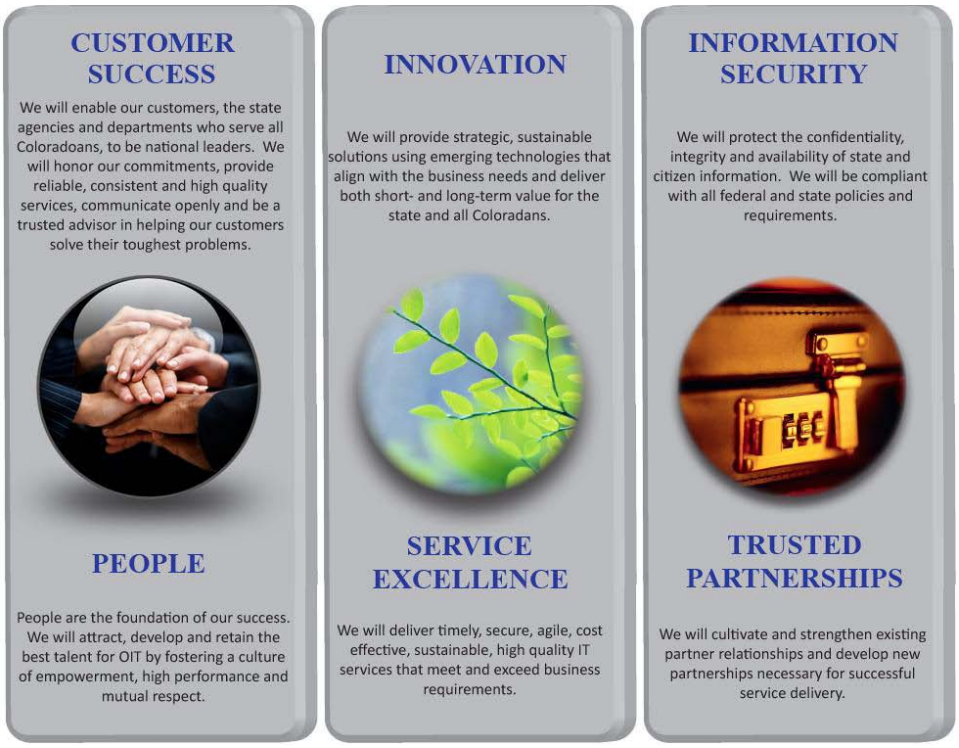
- Develop and update information security policies, standards, and guidelines for public agencies.
- Promulgate rules containing information security policies, standards, and guidelines.
- Ensure the incorporation of and compliance with information security policies, standards, and guidelines in the information security plans developed by public agencies.
- Direct and respond to information security audits and assessments in public agencies in order to ensure program compliance and adjustments.
- Establish and direct a risk management process to identify information security risks in public agencies and deploy risk mitigation strategies, processes, and procedures.
- Approve or disapprove and review annually the information security plans of public agencies.
- Conduct information security awareness and training programs.
- In coordination and consultation with the Office of State Planning and Budgeting and the Chief Information Officer (CIO), review public agency budget requests related to information security systems and approve such budget requests for state agencies other than the legislative branch.
- Coordinate with the Colorado Commission on Higher Education for purposes of reviewing and commenting on information security plans adopted by Institutions of Higher Education.
- Oversee incident response activities as well as the investigation of security breaches, and assist with the disciplinary and legal matters associated with such breaches as necessary and maintain authority to direct discontinuation of services from unsafe systems.
- Maintain relationships with local, state and federal partners and other related private and government agencies.

Within the Governor's Office of Information Technology (OIT), the CISO reports administratively to the Chief Technology Officer (CTO) who reports to the CIO. Information security duties and responsibilities for executive branch agencies are administratively divided between OIT's CTO and Chief Operations Officer (COO). While the CISO maintains responsibility for information security governance, architecture, risk, and compliance, the COO is responsible for overseeing day-to-day security operations, including access provisioning, network and endpoint security monitoring and administration, threat and vulnerability management, and computer forensics and incident response.

OIT Mission and Priorities

It's important that **Secure Colorado** aligns with OIT's mission and priorities, which in turn are aligned with the Governor's strategic plan. Protecting residents' data is required to meet OIT's value proposition to enable the effective, efficient and elegant delivery of government services through trusted partnerships and technology. OIT is committed to a set of core priorities, one of which is specifically focused on information security:

- Customer Success
- People
- Innovation
- Service Excellence
- Trusted Partnerships
- ***Information Security*** –ensuring the security, integrity, privacy and availability of information and systems



Colorado Information Security Program Vision and Mission

The following are the vision and mission for the Colorado Information Security Program, including a description of our philosophy for tackling the State's information security challenges and assuring the confidentiality, integrity, and availability of state networks, systems, and data.

Vision

Cost-effectively preserving the confidentiality, integrity, and availability of state and residents' data through the innovative use of the right people, processes, and technology.

Mission

Enable the State of Colorado to achieve its business objectives by maintaining an appropriate level of information security risk that promotes innovation, the effective use and adoption of information and information technologies, and fosters citizen engagement and e-commerce.

Team Slogan

Together, enabling state government operations through the efficient, effective, and elegant application of information security.

Philosophy Toward Information Security and Risk Management

Our philosophy describes how we approach the development of solutions for securing Colorado's information and systems. The Colorado Information Security Program will perform its work according to the following principles:

1. Offense must inform defense
2. Security must be built into business processes and IT systems from the start
3. Cyber threats are mitigated through the right combination of people, processes, and technology
4. Our security efforts must first be focused on our high value targets
5. Complexity is the enemy of security
6. Automated controls are superior to manual controls
7. Security drives compliance and not vice versa
8. Security must be efficient - only those security resources necessary to achieve our mission are acquired and deployed
9. Security must be effective - security must be results-oriented and anticipated outcomes measured, tracked, and compared to the resources expended
10. Security must be elegant – the most effective controls and security solutions are those that are transparent to the business and end user and seamlessly integrate with the State's business processes and existing technology

Section II – Strategic Priorities

> Every soldier must know, before he goes into battle, how the little battle he is to fight fits into the larger picture, and how the success of his fighting will influence the battle as a whole.
> -- Bernard Law Montgomery

Secure Colorado establishes a roadmap for improving cyber security in Colorado over the next three years. This plan was developed in cooperation with the Colorado Information Security Advisory Board (Board) – see Appendix A for Board Membership. The Board was formed by the CISO in 2012 to assist in the development of strategic and tactical plans aimed at reducing the State of Colorado's risk levels and improving the confidentiality, integrity, and availability of the information entrusted to the State.

Secure Colorado includes four strategic goals supported by 18 strategic initiatives. These goals and initiatives are based on foundational information security principles that are designed to be relevant for years to come. Supporting operational initiatives will be developed annually and included in the OIT Playbook, which can be found on the OIT's website – www.colorado.gov/oit. These operational-level initiatives will be the Colorado Information Security Program's primary focus for that specific fiscal year and will be aligned with one or more of **Secure Colorado's** strategic goals and initiatives.

To maintain its relevancy, **Secure Colorado** will be reviewed annually by the CISO, in conjunction with the Colorado Information Security Advisory Board and OIT Executive Leadership Team.

Protection

Goal # 1 – Protect State of Colorado information and information systems to assure that the confidentiality, integrity, and availability of all information is commensurate with mission needs, information value, and associated threats

STRATEGIC INITIATIVES

Initiative # 1.1 – Design, build, and operate resilient and self-healing systems and networks that are capable of resisting current and emerging cyber security threats.

Initiative # 1.2 – Recruit, develop, and retain a motivated, professional, and knowledgeable information security workforce.

Initiative # 1.3 – Design, build, and operate the necessary tools, techniques, and procedures to maintain "24/7" information security situational awareness of all state networks, systems, and data.

Initiative # 1.4 – Develop and maintain information security policies, standards, and guidelines that are relevant, adaptable, and cost-effective.

Initiative # 1.5 – Promote the understanding and acceptance of information security concepts and practices throughout state government.

Initiative # 1.6 – Equip state information technology professionals with the tools, knowledge, and skills to design, build, and operate secure applications and systems.

Initiative # 1.7 – Develop, document, and socialize an information security architecture that (1) aligns with the CTO's strategy, known as "The Compass: Enterprise Architecture 2011-2014," (2) transparently integrates security processes into next-generation state networks and systems, and (3) anticipates and addresses future threats.

Initiative # 1.8 – Develop and maintain a statewide incident response and computer forensic capability that is able to (1) quickly identify and isolate security incidents, (2) recover impacted systems and business processes, and (3) when feasible, identify and prosecute those attacking state systems.

Initiative # 1.9 – Develop, document, and implement a standardized risk management framework for accurately and uniformly assessing and managing the risk to the confidentiality, integrity, and availability of state systems and networks.

Research and Development

Goal # 2 – Research, develop, and employ innovative and sustainable information security solutions to address Colorado's cyber security challenges

STRATEGIC INITIATIVES

Initiative # 2.1 – Actively leverage federal government, private sector, and academic research and development of advanced cyber security tools and capabilities to assure the confidentiality, integrity, and availability of state systems and data.

Initiative # 2.2 – Rapidly evaluate, build, and deploy cutting-edge information security technologies to outpace emerging threats.

Initiative # 2.3 – Identify, evaluate, and share information on the threats and vulnerabilities impacting state government to support future research and development efforts.

Initiative # 2.4 – Use data and information to research and analyze cyber security trends.

Partnerships

Goal # 3 – Develop and foster key partnerships to improve information sharing, reduce information security risk, and promote innovation and collaboration

STRATEGIC INITIATIVES

Initiative # 3.1 - Develop and formalize new partnerships with academic institutions, the private sector, and Colorado state and local governments to share information security threat intelligence, research and development efforts, and best practices.

Initiative # 3.2 – Maintain active participation with the relevant organizations such as the National Association of State CIOs (NASCIO) Privacy and Security Committee, Multi-State Information Sharing Analysis Center (MS-ISAC), Colorado Government Association of Information Technology, National Institute of Standards and Technology, the SANS Institute, and other relevant organizations.

Initiative # 3.3 – Promote discussions and cooperative engagements that will enhance cyber security for all Colorado residents including partnering with the Colorado Department of Public Safety, Federal Department of Homeland Security, and the Colorado National Guard in achieving the cyber security objectives of the Colorado homeland security strategy.

Compliance

Goal # 4 – Comply with applicable information security and data privacy laws and regulations

STRATEGIC INITIATIVES

Initiative # 4.1 – Continuously assess and evaluate State systems and networks.

Initiative # 4.2 – Conduct targeted, technical audits to identify and correct non-compliance with State Cyber Security Policies and applicable federal laws and regulations.

Initiative # 4.3 – Partner with executive branch agencies and other public agencies to assist them in preparing for and responding to information security-related audits.

Section III –Strategic Success Measures

Metric Name	Target	Reporting Frequency	Description
Goal # 1 - Protect State of Colorado information and information systems to assure that the confidentiality, integrity, and availability of all information is commensurate with mission needs, information value, and associated threats			
Percentage of State Systems Actively Managed by Security	100%	Monthly	Percentage of total state systems actively managed and protected (in near real-time) by the Colorado security team.
Composite Information Security Risk Index	< 10	Quarterly	Overall, enterprise-level cyber security risk rating - based on current threats, asset value, and implemented security controls, ranked on a scale from 1 to 100 with 100 being extreme risk and 0 being no risk.
Mean Time from Incident Detection to Containment	< 60 min.	Quarterly	Measures the average length of time necessary to contain a security incident and restore impacted services.
Percentage of Employees Completing Security Training	95%	Monthly	Percentage of state employees completing security training, including new employee training, annual refresher training, and technical security training.
Goal # 2 - Research, develop, and employ innovative and sustainable information security solutions to address Colorado cyber security challenges			
Percentage of State IT Expenditures Spent on Information Security	5%	Annual	Measures the percentage of IT expenditures utilized to design, build, and implement innovative and sustainable information security solutions.
Number of Emerging Cyber Security Product Evaluations Completed	3	Annual	Represents the number of emerging security product reviews completed annually to address emerging cyber security challenges.
Mean Time from Identified Need to Recommended Solution	< 12 days	Annual	The average number of days elapsed between the identification of a cyber security need to a recommended solution.
Goal # 3 - Develop and foster key partnerships to improve information sharing, reduce information security risk, and promote innovation and collaboration			
Number of Active Information Sharing Agreements	Tracking Only	Annual	Tracks the number of partners for which the security program shares threat and vulnerability information
Number of Security Thought / Evaluation Products Shared with Partners	3	Annual	Number of written cyber security product evaluations and “thought” papers shared with partners

Goal # 4 - Comply with applicable information security and data privacy laws and regulations			
Number of Managed Security Audit Findings	Tracking Only	Quarterly	Tracks the total number of security-related audit findings actively being managed by the security team.
Percentage of Overdue Security Audit Findings	5%	Quarterly	Percentage of security-related audit findings that are not implemented and are past their agreed-to implementation date.
Average Number of New Security Audit Findings Per External Audit/ Inspection	< 8	Annual	The average number of new security-related audit findings per external party audit.

Appendix A – Colorado Information Security Advisory Board

Colorado Information Security Advisory Board 2012-2013	
Alan Paller, Co-Chair Founder and Director of Research SANS Institute	Rick Dakin, Co-Chair Co-Founder and CEO Coalfire Systems
Kent Lambert, Member State Senator, District 9	Paul Underwood, Managing Partner and COO Emagined Security
Dan Jones, Assistant Vice President and CISO University of Colorado System	Brian Tillett, Chief Security Strategist Symantec
Tim Erlin, Director, Product Management, Security, and IT Risk Strategist, nCircle	Robert Rudolff, Assistant Vice Chancellor and CISO University of Denver
John Conley, Executive Director Statewide Internet Portal Authority	Steve White, Director, Cybersecurity Practice, Enterprise Services, Microsoft Corp.
Eran Feigenbaum, Director of Security Google	Mark Lewis, Security Engineer McAfee
Sheryl Rose, Vice President, CISO Catholic Health Initiatives	Trevor Timmons, CIO Colorado Secretary of State's Office
Colonel Gregory A. Miller, Deputy Chief of Staff Colorado Army National Guard	Jeff Franklin, CISO State of Iowa
Eric Bergman, Policy and Research Supervisor Colorado Counties, Inc.	Randall J. Romes, Principal CliftonLarsenAllen, LLP
Tim Gama, Program Coordinator Pueblo Community College	Len Meyer, Director of Infrastructure Services Governor's Office of Information Technology
Alfritch Anderson, Security Operations Manager Governor's Office of Information Technology	Craig Fuller, IT Asset Manager Governor's Office of Information Technology
Rick Matsumoto Director of Enterprise Applications Governor's Office of Information Technology	Barbara Gilmore Deskside Support Services Manager Governor's Office of Information Technology
Heather Copp, Deputy Director Colorado Department of Revenue	Erika Bohl, Chief Privacy Officer Department of Health Care Policy and Financing
Kathleen Foo, Chief Privacy Officer Colorado Department of Human Services	Dan Krug, Analyst Governor's Office of State Planning and Budgeting
Stephanie Donner, Deputy Legal Counsel Office of the Governor	Brandon Rattiner, Denver Metro Regional Director Office of Senator Mark Udall
Dana Reynolds, Director of Preparedness Colorado Department of Public Safety	Karl Wilmes, Deputy Director Colorado Bureau of Investigation