Costs are High for Security Incidents

Data Breach

$3.86 million = average cost of data breach

$148 average cost per lost or stolen record

Major Malware Attack

$2.4 - $5 million = average cost of a major malware attack

Why might it cost more than a data breach?

- 25% of total — attributable to system downtime
- 30% of total — attributable to end user productivity loss.

Statistics from Ponemon & Symantec (2018)
Security Incidents are Common Occurrences

Ransomware attacks have doubled in the last year
- the majority of infections are enterprises (81%)

Email is a necessary evil
- 92% of malware is delivered by email
- 55% of email is spam (consistent year-over-year)
- 48% of malicious email attachments are office files - up 43% from last year!

Statistics from Ponemon & Symantec (2018)

Cybersecurity

Case Study: Having a security program in place makes a huge difference!

<table>
<thead>
<tr>
<th>Security Program in Place</th>
<th>Inconsistent or Non-Existent Security Program</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Colorado CDOT: SamSam - February 2018</strong></td>
<td><strong>Atlanta: SamSam - March 2018</strong></td>
</tr>
<tr>
<td>$1.7 Million total cost</td>
<td>$17 Million+ total cost</td>
</tr>
<tr>
<td>&lt; 8 weeks recovering</td>
<td>&gt; 6 months recovering</td>
</tr>
<tr>
<td>4 weeks offline</td>
<td>&gt; 3 months offline for ¼ of the services</td>
</tr>
<tr>
<td>No production data loss</td>
<td>Significant data loss including 10 years of public safety data</td>
</tr>
<tr>
<td>No resident impact</td>
<td>Resident impact affecting up to 6 million people</td>
</tr>
</tbody>
</table>
Cybersecurity

"If there is a playbook for bouncing back from a ransomware incident, it might resemble the one the Colorado Office of Information Technology developed last year when that state's transportation agency had its own run-in with the SamSam virus."

StateScoop, March 22, 2019

History of Cybersecurity - Colorado

<table>
<thead>
<tr>
<th>2006</th>
<th>2008</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
</table>
What We Do for Executive Branch Agencies

Statewide Security Policies and Strategy
Enterprise IT Risk Management
Proactive Security
  • Assessments
  • Vendors
  • Projects
Security Awareness
Operational Security
Security Monitoring and Incident Response

What We Do for Non-Consolidated Agencies

Statewide Security Policies
Review Agency Cyber Security Plan
  • Annual submission required
Monthly Security All-Hands Meetings
Provision of Consulting and Guidance as Requested

Non-Consolidated Agencies:
  • Judicial
  • Legislative
  • Secretary of State
  • Higher Education
  • Department of Education
  • Department of Law

Colorado Cyber Security Program - June 2019
Budget Progression and Accomplishments

**Secure Colorado program implemented!**

- **2012**
  - No security consistency between agencies
  - No budget for improvements

- **2014**
  - Next Gen perimeter firewall
  - Standard endpoint security toolset
  - Security improvements underway

- **2016**
  - 2-step verification for Google
  - Identity & Access Mgmt Toolset deployment underway

- **2018**
  - Next Gen endpoint security toolset
  - Firewall standardization across agencies in-progress
  - >600 audit recs implemented

- **2020**
  - Accelerating in-progress security improvements
  - Additional controls for privileged accounts
  - Cloud governance

- **2021**
  - Sustaining & maintaining processes, tools, FTEs & salaries implemented in 2020
  - Continuing security improvements

*of overall statewide IT spend, estimated @ $350 million annually*

Colorado CyberSecurity Program - June 2019
Cybersecurity Spend Compared to Other States

Most states indicate that their cybersecurity budget is now 1 to 3 percent of their total IT budget.

What percent of your state's enterprise IT budget is allocated to enterprise cybersecurity (all executive branch agencies)? (50 respondents)

<table>
<thead>
<tr>
<th>%</th>
<th>2018</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>0%</td>
<td>6%</td>
</tr>
<tr>
<td>0-1%</td>
<td>12%</td>
<td>18%</td>
</tr>
<tr>
<td>1-2%</td>
<td>30%</td>
<td>27%</td>
</tr>
<tr>
<td>2-3%</td>
<td>12%</td>
<td>12%</td>
</tr>
<tr>
<td>3-5%</td>
<td>12%</td>
<td>12%</td>
</tr>
<tr>
<td>6-10%</td>
<td>10%</td>
<td>0%</td>
</tr>
<tr>
<td>N/A</td>
<td>18%</td>
<td>25%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
<td></td>
</tr>
</tbody>
</table>

State of Colorado = 3.6% of overall statewide IT spend


Colorado CyberSecurity Program - June 2019
Secure Colorado: Colorado's Cybersecurity Strategic Plan

Quick and sustainable risk reduction
National Association of State CIOs (NASCIO)

Innovation in Security
Center for Digital Government

Outstanding business value and thought leadership
CIO Magazine

Secure Colorado chosen as a cybersecurity strategy model for the National Governors Association Policy Academy
Secure Colorado: Framework

Basic
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Framework: 20 Critical Security Controls for Effective Cyber Defense

Colorado CyberSecurity Program - June 2019
Considerations for Establishing Security Priorities

- Evolving business needs
- Threat landscape
- Security gaps
- Innovation
- Funding gaps & maturity
- CO Information Security Advisory Board Input

Annual Security Priorities

Secure Colorado - Focus for 2020

Identity and Access Management
- consistency in how user accounts are managed and fewer audit findings

Better controls over Privileged Accounts
- reduce the risk of an attacker using a privileged account which could compromise an agency

Cloud governance team
- ensure more secure adoption of cloud services and ensuring data stored in cloud services is appropriately protected

Audit remediation
- fix known weaknesses in our environment
Secure Colorado - Focus for 2020

Faster detection and response for security events
- resulting in prevention of successful attacks and minimization of impact

Upgrade agency firewalls
- completion of this project will ensure all agencies are protected by our standard next-generation best-in-class firewall

Consistent patching and security updates across all environments
- resulting in a more hardened environment that is less susceptible to attack and fewer audit findings

Salary adjustments
- to retain hard-to-fill positions

Challenge: Cybersecurity Workforce
Filling the Cybersecurity Workforce Gap

Veterans Transition Program
- 9-month paid internships
- 2 levels of VTP-interns
- budgeted for 10

Cyber Patriots
- High school and Middle school teams
- Cyber protection techniques

Women in Security
- Local Denver group
- ~100 women at every event!

Girls Go CyberStart
- Free for girls in grades 9-12
- Discover cybersecurity interest and talent

Questions
Enterprise Identity Management Program

The program supports a centralized system for secure access, authentication, authorization, and user account information. It drives efficiency by replacing manual processes with automated identity provisioning, and managed role-based access to administer systems that enforce least privilege best practices, and overall identity lifecycle maintenance.
Colorado Identity & Access Management Program Compared to Other States

Thirty-three states have either established an enterprise IAM solution or plan to perform a product selection

<table>
<thead>
<tr>
<th>2018</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, all agencies under the governor's jurisdiction are covered</td>
<td>18%</td>
</tr>
<tr>
<td>Yes, partial list of agencies under the governor's jurisdiction are covered</td>
<td>24%</td>
</tr>
<tr>
<td>No, but performing or plan to perform a product selection</td>
<td>24%</td>
</tr>
<tr>
<td>No, but plan to implement</td>
<td>22%</td>
</tr>
<tr>
<td>No, do not plan to implement</td>
<td>8%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
</tr>
</tbody>
</table>


State of Colorado Implementing for all of Governor's Jurisdiction
Enterprise Identity Management Services

Ensuring Access, Security and Compliance
- Automated account provisioning/de-provisioning
- On-demand audit and reporting
- 24x7 self-service password reset and password unlock
- Role Based Access Control
- Privileged Access Management
- 2 Factor Authentication
- Single Sign-On

Value
- People
- Process
- Security & Audits
- Cost

Identity & Access Management Case Study

<table>
<thead>
<tr>
<th>Past</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 days to onboard, offboard, manage access</td>
</tr>
<tr>
<td>4000+ Provisioning Requests per month supporting up to 70k users (executive branch, non-executive branch and external users)</td>
</tr>
<tr>
<td>529 privileged accounts</td>
</tr>
<tr>
<td>Lack of role-based access</td>
</tr>
<tr>
<td>IT staff managing customer password resets</td>
</tr>
<tr>
<td>5,280 password resets per month</td>
</tr>
<tr>
<td>Lack of visibility, ownership or logging of privileged accounts</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Present</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same day, Immediate or Planned (network, email, ITSM, PAM)</td>
</tr>
<tr>
<td>Standardized role-based access established (30k users)</td>
</tr>
<tr>
<td>53 privileged accounts</td>
</tr>
<tr>
<td>Governed application role-based access</td>
</tr>
<tr>
<td>24x7 self-service offering for both password management and provisioning</td>
</tr>
<tr>
<td>Ability to auto discovery privileged accounts and safeguard them</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional system integration to improve user experience, centralize access management, and remediate audit findings</td>
</tr>
<tr>
<td>Joint Agency Interoperability</td>
</tr>
<tr>
<td>All privileged accounts managed in vault with session recording and 2FA</td>
</tr>
<tr>
<td>Mature standards by requiring application integration with One Identity Manager and/or Active Directory</td>
</tr>
<tr>
<td>Enable 2FA on all privileged accounts and log activities performed</td>
</tr>
</tbody>
</table>

Colorado Cybersecurity Program - June 2019
Identity & Access Management Focus for 2020

Cloud Access Security Broker (CASB) - provide visibility to cloud application usage, adds compliance, threat protection, data security, and data loss prevention

Identity Analytics & Risk Intelligence (IARI) - reduce risk and attack surface before bad behavior impacts business by eliminating unnecessary or dormant entitlements before abuse or exploitation

Data and Access Governance - review and control access to unstructured data in files, folders, shares and SharePoint and put the control in the hands of the business data owner

Additional application integration for HRWorks (Workday) and critical and essential applications

Other FY19 accomplishments

- ZFA on all 11k remote users
- Single Sign-On
- Citizen Identity Access Management - myColorado

Questions