



## Securing Colorado

Deborah Blyth, State of Colorado Chief Information Security Officer

May 2018





# AGENDA

Governor's Office of  
Information Technology and  
CISO Role

Cybersecurity Strategy:  
Secure Colorado

Ransomware at CDOT

Mitigating the Cybersecurity  
Workforce Gap

# Cybersecurity at the State of Colorado

- Providing security governance and operations for 17 Executive Branch agencies
- Managing a \$12.6 million annual cybersecurity budget
- Budget requests supported by Office of State Planning and Budgeting (OSPB) and approved by:
  - Joint Technology Committee (JTC)
  - Joint Budget Committee (JBC)
  - General Assembly
  - Governor
- Regular presentations to the JTC and Legislative Audit Committee (LAC)
- 1,200 agency applications
- >8.4 million statewide security events monitored by Security Operations daily



# State of Security: Colorado today

Colorado's cybersecurity program is:

- > 4% of statewide IT spend,
- one of the IT Strategic Goals,
- recognized as being very successful!

Delivering effective solutions and reliable customer service



Securing Colorado through innovation



Ensure all Coloradans have access to reliable, cost-effective broadband internet



Strengthening Colorado's technology landscape



Advancing a culture of employee support and collaboration



# Secure Colorado: Colorado's Cybersecurity Strategic Plan

Secure  
Colorado:

*To reduce the  
state's  
exposure to  
data breaches  
and cyber  
attacks*

*To justify  
ongoing  
budget for  
security  
improvements*

Protect Information and Systems

Research and Development

Partnerships

Compliance

Framework:

20 Critical  
Security Controls  
for Effective  
Cyber Defense  
(Center for Internet  
Security)



# Secure Colorado - Program Accomplishments

- ✓ Security Tools in Place
- ✓ Risk Reduction
- ✓ Two-Step Verification
- ✓ Audit Remediation
- ✓ Quarterly Security Awareness Training
- ✓ Best Practice & Leading-Edge Security
- ✓ Secure Applications



# Considerations for Establishing Security Priorities



# Ransomware Security Incident

## THE DENVER POST SamSam virus demands bitcoin from CDOT, state shuts down 2,000 computers

Colorado investigators call in FBI, work through the night



**Ransomware attack on CDOT might  
have been stopped if it was one week  
later**



# State of the Cybersecurity Workforce

## State of Cyber Security 2017 Workforce Trends and Challenges

[www.isaca.org/state-of-cyber-security-2017](http://www.isaca.org/state-of-cyber-security-2017)

### Hiring Challenges Persist

55%



indicate that open positions take at least **THREE MONTHS** TO FILL.



**32% OF ENTERPRISES** report that the time to fill cyber security and information security positions is **SIX MONTHS OR MORE**.

MORE THAN **1 IN 5**

organizations get **FEWER THAN 5 APPLICANTS** for an open cyber security position.



ONLY **13%**

GET **20 OR MORE APPLICANTS**.

### HIRING STATUS

Many are **UNABLE TO FILL** open cyber security positions in their enterprises:

IN THE US:

**59%**

CAN FILL OPENINGS

**14%**

DON'T KNOW



### Skills and Certifications in Demand

37%



SAY **FEWER THAN 1 IN 4** candidates are qualified

55%

SAY **PRACTICAL HANDS-ON EXPERIENCE** is the most important qualification for a cyber security candidate.



CLOSE TO **70%**

of hiring enterprises require a **SECURITY CERTIFICATION** for open cyber security positions.

SOURCE: ISACA's State of Cyber Security 2017: Current Trends in Workforce Development  
[www.isaca.org/state-of-cyber-security-2017](http://www.isaca.org/state-of-cyber-security-2017)

© 2017 ISACA. All rights reserved.



# Filling the Cybersecurity Workforce Gap


## Veterans Transition Program

- 9-month paid internships
- 2 levels of VTP-interns

## 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

- For girls in grades 9-12 
- Discover cybersecurity interest and talent



Altona Middle School Cyber Patriots



# Security Analytics and Automation

Security Analytics to Highlight Anomalies

Incorporating Threat Intelligence into Security Tools

Automating Detection and Response Activities



# Additional Resources

Secure Colorado:

<http://oit.state.co.us/securecolorado>

Critical Security Controls for Effective Cyber Defense:

<https://www.cisecurity.org/critical-controls.cfm>

My email: [deborah.blyth@state.co.us](mailto:deborah.blyth@state.co.us)