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!
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

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

Innovation

- Evolving business needs
- Threat landscape
- Security gaps
- Funding gaps

Annual 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

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.

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 cybersecurity candidate.

Hiring Status
Many are unable to fill open cybersecurity positions in their enterprises:
- US: 27%
- Europe: 30%
- Asia: 22%

Source: ISACA's State of Cyber Security 2017: Current Trends in Workforce Development
© 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
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