ANDY HANKS
CHIEF INFORMATION SECURITY OFFICER
STATE OF MONTANA

Interim Budget Committee
December 15, 2021

Cybersecurity

ANDY HANKS
CHIEF INFORMATION SECURITY OFFICER
STATE OF MONTANA
• Cybersecurity Enterprise Rate Background
• Cybersecurity Enterprise Rate Breakdown
• Evaluating Cybersecurity Costs
• Outline of the Information Provided During Session
• Conclusion
Since 2010, State CISOs have reported the lack of sufficient funding as the number one barrier to addressing cybersecurity challenges.

A dedicated cybersecurity budget provides more visibility.

Monitoring and measurement of enterprise cybersecurity investments.

Federal and state cybersecurity mandates, legislation, and standards with funding assistance result in more dramatic progress than those that are unfunded.

Federal funding for security requirements and controls.
CYBERSECURITY ENTERPRISE RATE - Breakdown

- 20/21 Services transferred from ESA: $4,321,538
- Increase for 20/21 Services: $850,423
- HB2 Operating: $1,645,382
- HB2 PS: $465,610
- Virtual Server: $301,446
- Live Storage: $95,189
- Tenable Increase: $153,750
- Security Awareness Training: $104,550
- Palo Auto Focus: $56,375
- E-Gov Identity Management: $57,378
- Application Development Hours: $24,000
- PS Increase: $80,000
- Total CESA: $8,155,640
EVALUATING CYBERSECURITY COSTS

• Business Perspective

• Cost Avoidance

• Insurance

• Other (e.g., data-driven modernization efforts)
The average costs of data breaches is increasing
  - The average cost of data breaches increased by $380k to $4.24m since last year
  - This 9.8% increase is the largest year-over-year increase in seven years

The average cost per record lost is $161 and $181 per record containing PII
  - A breach of a statewide database would cost approximately $161m
  - A breach of a statewide database containing PII would cost approximately $181m (44% of data breaches)

The time to identify and contain data breaches is increasing
  - Identifying data breaches early is critical to limiting scope and impact which reduces the associated costs
  - It takes 287 days to identify (212 days) and contain (75 days) a data breach, 7 days longer than last year
  - If a data breach occurs on January 1, then it would not be contained until October 14

The frequency of data breaches is increasing
  - There were 1,108 data breaches reported in 2020
  - There have already been 1,209 data breaches reported in 2021 (17% increase year-over-year)

The most common initial attack vectors leading to data breaches are compromised credentials (20%), phishing (17%), and cloud misconfiguration (15%)
  - Cybersecurity investments are made based risk assessments and current threat environment
  - Risk-based investments ensure funding is applied to gain the most value to protect citizen data
OUTLINE OF INFORMATION PROVIDED DURING SESSION

2021.01.02 Budget Presentation.pdf
• a description of 2019 HB2 Montana Cybersecurity Enhancement Project (MT-CEP) projects, their benefits including metrics and statistics, and the potential impacts of proposed reductions to cybersecurity funding in the 2021 session.

CESA Descriptions v4.pdf
• a description of the enterprise services and costs included in the Cybersecurity Enterprise Rate.

Committee Questions.pdf
• responses to subcommittee questions about SITSD’s budget presentation.

Cybersecurity Enterprise Rate.pdf
• a visual of the cost categories (Vendor Costs, Personal Services, and Internal Costs) that make up the Cybersecurity Enterprise Rate.

MT-CEP2 Budget Crosswalk v3.pdf
• a description of the 2019 HB2 Montana Cybersecurity Enhancement Project (MT-CEP) detailing which projects used new budget and which projects augmented existing budgets.
CONCLUSION/NEXT STEPS

• Enterprise Risk Assessment (In Progress)

• Metrics Program Improvements

• Federal Programs

• Questions?