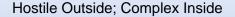
Economic Affairs Interim Committee Identity Theft Overview Government IT Presentation

Agenda

•It's a hostile world outside; complex inside •Responsibilities within the State •Key Issue

•Actions completed/underway/anticipated





- Threats from the outside
 - Unauthorized attempts to enter the State network: 1.5 Billion successful: 0 CY2004
 - Virus exposures: 1,540,000
- "infections": 36 workstations • Complexity challenges from the inside
 - Vast amounts of data: est. 50 TB (trillion characters)
 - Personal data scattered throughout the State
 - 758 server computers in 211 sites
 - About half housed in 55 sites/"data centers" in

Helena area





Key Issue

- Attention has been focused on prevention of a breach; less focus on response
 - State has done a very good job preventing security breaches
 - Must assume a breach will occur ... we are not adequately prepared to respond when it occurs

Actions

Completed/Underway/Anticipated

- PC Disposal ("cleansing") Policy/Process
 - Completed Policy & process in response to audit
 Underway working on more effective process
- Continue prevention improvements
- Breach response policies to assure consistent, appropriate responses
 - Anticipate significant effort in coming months
 - Align with Security Breach law (MCA 30-14-1704)
 (Effective March 1, 2006)
 - Leverage CSIRT into agency breaches
 Best practices NASCIO has published

 - guidelines for policy creation

