Current Threats

Sean Rivera
Bureau Chief – Information Security
srivera@mt.gov
DOA-SITSD
08 March 2017
Email & Ransomware Distribution

• 2016 – Ransomware was present in 1 out of 5 emails
• Most popular variants –
  • Locky
  • Petya
  • Cryakl
  • Shade
• Spam accounted for 58% of all email
Data Breaches in 2017

- 248 Data Breaches through Feb 28, 2017
- Medical/Healthcare – 26.7% accounting for 560k records
- EDU – 17.1%; 28k records
- GOV/MIL – 5.4%; 40k records
- Since 2005, ITRC tracked 7,139 breaches and 889mil records
Typo Leads to Turmoil

- Amazon’s Simple Storage Service (S3) suffered outage on Feb 28
- Attempt to perform debug maintenance let to a mistyped command, removing more servers than intended
- Other examples of typos
The Effectiveness of Removing Admin Rights from Workstations

- A study suggested that 94% of critical MS vulnerabilities released during 2016 could be fixed by removing admin rights

- 530 vulnerabilities total; 189 critical

- 100% of Edge/IE vulns were mitigated by removing admin rights