Speaking outline

* Introduction
  + 62% of small-medium sized businesses are affected by ransomware attacks (Elizabeth one of them)
  + Purpose – investigate necessity of having robust vs inexpensive security system
  + Two Approaches, Robust Vs. Inexpensive
* Robust Security Approach
  + Ransomware/Email Fraud
    - Large amount of money lost this way
    - Human factor involved most of the time. (95%)
  + Potential losses
  + Reputation
  + People stop buying at websites that are breached
  + Regulations
* Inexpensive Security Approach
  + Costs and Savings
  + Chances of Data Breaches
  + Employee Equipment Software purchases
  + Anti-Virus
  + Two-Factor
* Conclusion
  + Chances are high enough of a breach that Robust should be implemented
  + Savings do not outweigh the ramifications of having a breach
  + Reputation sinks if breach does happen
* Recommendation
  + Hire outside company such as NINJIO for data security purposes
  + OR hire own set of data security engineers
  + Two-factor along with employee lockdown applications
  + Training course so human component in breach is minimized
  + Monitor employees (maybe?)