1. Give an overview of what the breach was and the motivations behind it.
   1. In 2015, the U.S. Office of Personnel Management had their data breached which included sensitive confidential information including SSNs of 21.5 million individuals of former and current government employees.
2. Explain where the “tech flaws” were, and how hackers were able to breach their system.
   1. The attacker posed as an employee of KeyPoint Government solutions.
3. What has the company done to protect against that vulnerability since?
   1. Much has not been sent about what the government has done to protect against the vulnerabilities. However, there were services that the government introduced to individuals that were affected.
      1. Full service identity restoration, which helps to repair your identity following fraudulent activity.
      2. Identity theft insurance, which can help to reimburse you for certain expenses incurred if your identity is stolen.
      3. Continuous identity and credit monitoring