# Cloud Risks

**Service/ Technical Risks**

1. SLAs
   1. Are SLAs well defined in your contract?
   2. **Amazon’s Cloud Crashed on 4/21/2011 (example)**
2. Third Party – Is your provider sub-contracting work out?
   1. Are Cloud providers using other clouds?
3. Lack of Standards
   1. Will providers offer regular risk assessments?
   2. Are you permitted to audit?
4. Data Segregation
   1. Will data be stored separately from competitors?

**Business Risks**

1. Is the provider financially viable?
   1. What happens if they go out of business?
   2. Ownership Issues – Who owns the data, you or your provider?
   3. Proper Return and Disposal of assets including backups.
      1. If something happens, you may not be entitled to backups.

**Legal Risks**

1. 4th Amendment does not apply to Cloud Computing.
   1. **Dec 2010 FBI raided a Dallas Carrier and seized cloud servers (example).**
2. Expectation of Privacy
   1. As soon as you go to Cloud you may relinquish your rights.
3. What laws apply?
   1. Local Legal System – Your rights are only as good as the where you live. Related to the local legal system is where your provider located and what laws would take precedent?
   2. Cross Boarder Data Transfer - If your data is housed in another country, what laws apply?
4. Government can Subpoena the provider without prior notice to you.
5. Breach
   1. If one occurs, are they obligated to tell you?

**Four considerations:**

1. Check your contract. How much do you trust the provider to do the right thing?
2. What laws based on location of you, your data or provider takes precedent?
3. I think Cloud providers will become the next big Black Hat targets.
4. Bottom line - we are still responsible for whatever happens to our data.