

# Next Direction Technologies

---

## Can I Keep Secret Data in the Cloud?

Mike Danseglio, CISSP



# Agenda

---

- The value of data
- A plethora of cloud solutions
- How to decide



---

# The Value of Data



# Data as a Key Business Asset

---

- Many companies rate data as their most valuable asset
  - Regardless of company size
  - Regardless of business or industry
  - Regardless of volume of data



# Data Loss Is Unacceptable

---

- Loss of data today is akin to loss of facilities 10 years ago
- It destroys businesses
- It sometimes destroys entire industries



# Data Theft Is Even Worse

---

- Stolen data is often turned against the source
  - Extortion
  - Disclosure
  - Legal action
  - Compliance breach
  - Competitive advantage

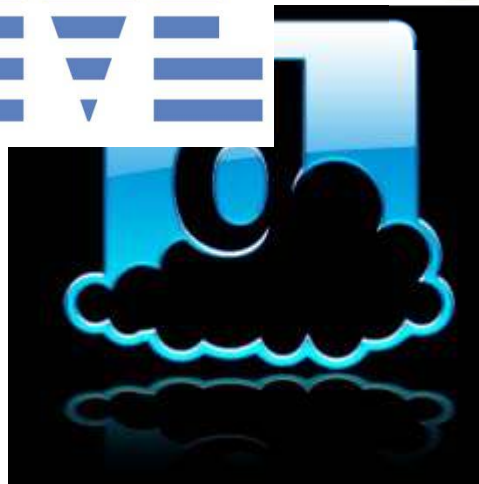
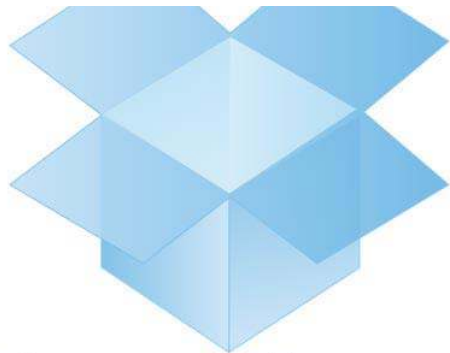
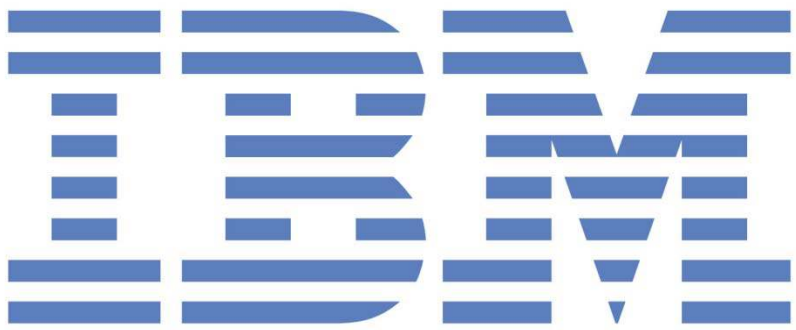


---

# A Plethora of Cloud Solutions



# The NASCAR Slide!



# Dropbox



# Decision Is Important

---

- Lack of standards may lock you in
- Commitment is hard to change
- Data loss and theft are not predictable



---

# How To Decide



---

# Three components in your decision...



tl;dr

---

1. Classify your data
2. Examine cloud providers
3. Uncertainty is insecurity



# Component #1: Classify Your Data

---

- Without classification you're not doing a good job
- A cloud solution supports (not creates) data classification



# Component #2: Examine The Cloud Providers

---

- Security documentation
- Service level agreements
- Insurance and assurance



# Security Documentation

---

- Audit reports relevant to your business needs
  - SAS 70
  - PCI
  - HIPAA



# Security Documentation

---

- Written policies and procedures
  - Data storage and retention
  - Compliance with legal mandates for disclosure
  - Data destruction
  - Data recovery
  - Human asset management (e.g. employee background verification requirements)
  - Data isolation





# Proof Is In The Pudding

---

- Ask for things like...
  - Network map
  - Encryption algorithms and key sizes used
  - Incident response plan
  - Failed audit documentation
  - Penetration test results



# Service Level Agreements

---

- Uptime
- Incident response
- Security compliance and timeliness



# Service Level Agreements

- A SLA for securing data must never include...



We have strict policy and technical access controls that prohibit employee access except in these rare circumstances.

A judge on Monday ordered a Colorado woman to decrypt her laptop computer so prosecutors can use the files against her in a criminal case.

you hereby grant Microsoft the right, to use, modify, adapt, reproduce, distribute, and display content posted on the service solely to the extent necessary to provide the service.

We may need your permission to do things you ask us to do with your stuff, for example, hosting your files, or sharing them at your direction. It also includes design choices we make to technically administer our Services, .... You give us the permissions we need to do those things solely to provide the Services.

When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display and distribute such content.

Apple may transmit your Content across various public networks, in various media, and modify or change your Content to comply with technical requirements of connecting networks or devices or computers.

by submitting or posting such Content ..... you grant Apple a worldwide, royalty-free, non-exclusive license to use, distribute, reproduce, modify, adapt, publish, translate, publicly perform and publicly display such Content on the Service solely for the purpose for which such Content was submitted or made available, without any compensation or obligation to you.

# Insurance and Assurance

---

- Underwriting policies
- Detailed guarantees
- Reputation

# Component #3: Uncertainty is Insecurity

---

- No documentation? OK, thanks. <CLICK>
- Oh, you don't provide security documentation because "hackers" will use it? OK, thanks. <CLICK>
- So you have really secure data through VPN but don't tell me if you encrypt the hard drives? OK, thanks. <CLICK>



# Security Assurance Is Critical

---

- All cloud storage providers know what data security is
- They've had ample time to
  - Secure assets
  - Document the security
  - Create a client-readable document



---

One recommended  
workaround...





---

If you want something done  
right, do it yourself!



# Working Around Lack of Confidence

---

- Secure the data yourself
- Do not give the keys to the cloud service provider
- Store the encrypted data



# Summary

---

- Yes, you absolutely can store and secure data in the cloud
- Selecting a provider is a pain in the \$\*%@!
- Researching the provider and solution will help avoid incidents



# Next Direction Technologies

---

Thank You!

