Bring Your Own Service

The Effects of Cloud Services on Compliance and Data Protection
Cloud Explosion

- Public cloud file sharing has exploded
- As of November 2012, Dropbox claimed to have 100,000,000 customers
Hey boss, can I use Dropbox?

Today

80% of companies at present do not allow cloud based file synchronization

14% of companies are satisfied with the controls that cloud based file sync services have in place

6% of companies are not satisfied but are going ahead anyway
Why not?

- Risk
- Control
- Complexity
Too bad! We’re doing it anyway

1 in 5 Employees use Dropbox for work!

What can we do about it?

• Given what end-users want:
  - Simplicity
  - Accessibility
  - Mobile support

• And what organizations need:
  - Control
  - Compliance
  - Security
What are the options?
Every business is different

CHOOSE YOUR OWN ADVENTURE

Cloud  Internal
To the cloud!
How does this affect data protection?

- You’re still responsible according to the Information Commissioner’s Office (ICO)
- Unless you are getting rid of all internally stored data, you’ll need to extend your controls and processes:
  - Backup & recovery
  - Entitlement reviews
  - Classification
  - Retention
  - Access auditing
  - Change control
What about compliance?

• Will vary by country

• Regulations can be complicated:

  - **EU** – 1995 Data Protection Directive (DPD) provides framework for separate laws in EU member nations
    - In 2012, EU introduced a revision to DPD to make laws more uniform – e.g., personal data identifiers vary by nation – and placed under single authority.

  - **US** – Personal data protection spread across different agencies (SEC, FTC, & HHS) and based on different legislation. Some key ones:
    - HIPAA, FCRA (Fair Credit Report Act), Gramm-Leach-Bliley, COPPA, Sarbanes-Oxley.
Key strategic decisions

• Which data are we moving? All, some, most?
• How do we *select* the data we’re going to move?
• Do we keep a duplicate copy inhouse?
• If so, which is the master copy?
• How do internal users synchronize with external users?
• How do we get the data back out of the cloud?
• How do we ensure compliance if we can’t monitor access?
5 phase process to ensure cloud readiness

1. Profile Data Use & Authorization Structure
   - Enable Audit Trail
   - Inventory Permissions

2. Identify Critical Data
   - Classify and Tag Sensitive, High Profile Data

3. Reduce Excess Access
   - Global Access Groups
   - Excessive Group Membership

4. Identify Key Users & Owners
   - Perform Entitlement Reviews
   - Formalize and Enforce Existing Processes

5. Define & Implement DG Policies
   - Authorization
   - Recertification
   - Handling Policies for Sensitive Data
Extend your existing infrastructure
69% want to keep data inhouse

IT plans to allow the use of cloud based file synchronization service

- No 69%
- Yes 31%
Why is that?

Concerns about cloud based file synchronization

26% worried about data loss or auditing access activity
What to look for in a solution

• Do I have to move my data?

• Can I use my existing Active Directory users/groups?

• Do I have to re-permission data?

• Can I quickly identify who has access to what?

• Can I monitor and audit who is touching data?

• Can I detect when sensitive data is being synchronized?

• Can I safely make changes to permissions?
Provide cloud *usability* using only existing infrastructure:

- There’s a folder
- You put stuff in it
- It syncs...

- *With your existing storage (NAS, file servers, SharePoint)*
- *Using Active Directory credentials*
- *Using your existing file system permissions*
Step 1: Login

Login with your domain credentials (Active Directory) and/or multi-factor authentication
Step 2: Collaborate

Your sync’d folders appear in explorer
Changes sync to your CIFS servers
See Sync Speeds and Notifications
Mobile Apps
Right click for instant Extra-net
Secure Collaboration with 3rd Parties

Set Permissions and Expiration dates
Share with partners, customers, vendors, and clients
Integrates with Data Governance Suite

- Use DatAdvantage to manage permissions
- Use DataPrivilege to automate authorization
- DatAnywhere activity is recorded by DatAdvantage

Click on a user or group to see everything they can touch.
Governance Suite – Real World Example:

Data owners can review DatAnywhere activity just as they would for any normal file share.
DatAnywhere Architecture

Windows File Systems
- MS Active Directory
- CIFS/NFS

UNIX/Linux
- DNS Edge server
- Sync Manager
- Sync Worker

NAS
- DNS Edge server
- Sync Manager
- Sync Worker

Windows
- Client authorization

Mac
- DatAnywhere Client

Smart Phone
- HTTPS

Tablet
Summary

• Cloud-style sharing and BYOD may be inevitable
• Organizations must choose a direction before the employees choose one for them
• Organizations have a choice between moving data to the cloud, or extending their existing infrastructure to provide cloud-style capabilities in-house
• Whichever direction your organization chooses, governance will be instrumental for secure collaboration
One more thing…

• Do any of these questions look familiar?
  - Who has and should have access to which folders?
  - What folders does a user/group have access to?
  - Who uses all this data & what are they doing?
  - Who does it belong to?
  - What’s stale?
  - What’s sensitive? And exposed?

• Are your authorization processes manual?
  - Granting access?
  - Reviewing access?

• Are retention and migration projects manual?
  - New NAS? New Domain? Cross platform?
  - How do we find the data we’re supposed to move? Delete?
**Governance, Risk, & Compliance**

- DatAdvantage
- DataPrivilege
- IDU Classification Framework

Ensures that only the right people have access to the right data at all times, access is monitored and abuse is flagged.

**Accessibility & Collaboration**

DatAnywhere

Extends existing infrastructure to provide private cloud file synchronization and sharing, while ensuring all data remains within the organization, and existing permissions are enforced.

**Electronic Retention**

Data Transport Engine

Intelligently automates data disposition, archiving and migration process using the intelligence of the Varonis Metadata Framework.
Thank you!