Best Practices for Hosted Data

Learning Goals

- Understand your "data universe" and treat it as such
- Appreciate the need for a complete and sustainable backup process
- Know the measures to avoid losing access to data
- Awareness of data migration options
- Consider privacy: honor "theirs", assert "yours"

5 Single-Word Notions about Data

- Unity: Know your data universe and treat it as such
- Redundancy: Have a complete and sustainable backup process
- Control: Take steps to avoid losing access
- Portability: Confirm your migration options in advance
- Privacy: Honor “theirs”, assert “yours”

Unity

- What lies at the center of your organization's technology world view?
  - Nonprofits tend to have a technology-centric view of information technology
  - It is much more appropriate and sustainable to have an information-centric world view
  - Well-maintained data will outlive specific tools
  - Technology is just a vessel for storing data

Unity

- Do you know where all your digital data is?
  - Remote data stores
    - CRM, eAdvocacy, web content, mailing lists
    - Web mail, Google Apps, Flickr, YouTube, blogs, Basecamp, Facebook/MySpace, etc.
  - Local data stores
    - Staff machines and laptops
    - File servers
    - Media – disks, thumb drives, Cds/DVDs, backup tapes
    - Cell phones and hand-held gizmos

Unity

- What to do?
  - Establish and maintain a data inventory
    - What is each asset?
    - Where is it?
    - How is it accessed, and who has access/control?
    - What software is needed/available to access it?
    - Is it sensitive? Are there privacy implications?
  - Have a process for updating the inventory as you create new information assets
    - Especially for hosted data

Redundancy

- Have a consistent, comprehensive backup process
  - Link your process to your data inventory
  - Archive hosted data to local backups
  - Archive local backups to off-site locations
  - Automate the process wherever possible
- Verify your backups are actually usable
  - Use multiple media types (optical vs magnetic)
  - Do test restores

Redundancy

- Three critical questions to ask
  - If your nonprofit workplace burned to the ground, is all your data safe and accessible elsewhere?
  - If one of your hosted services goes offline, do you have everything you need to migrate to a new service?
  - Are there any "single points of failure" in your organizational data map?

Control

- As an organization, you should have access to and control of your data
  - Externally, will each hosting service let you export your data on demand in a usable format?
    - Have you read the fine print on the license?
  - Internally, who has access to each data source/data asset?
    - Are there checks and balances?
    - What happens if they get hit by a bus?

Control

- Passwords are the keys to your data
  - Have an organizational password policy
    - Per data asset
    - Distinguish "strategic" data from "non-strategic"
    - Have passwords on all machines
  - Verify that you can do password recovery
    - Use aliases rather than individual email addresses for hosted account contact information
  - Change your passwords on a regular basis!
    - Whenever there is staff turnover

Control

- Beware "Free" accounts!
  - You have no control!
  - YAHOO Groups, Google everything, Flickr, etc
  - Avoid free account "sprawl"
- Free accounts can disappear any time
  - Beware the accidental and the insidious
  - If you depend on the service, pay the fee
- Make sure hosted documents and data get archived locally

Portability

- Data is your digital power
  - Your ability to migrate that data is crucial to your long-term effectiveness
  - Discuss migration options before signing on to any service
    - Verify vendor claims, via references or "by hand"
  - Insist on open data standards
    - CSV (comma separated values) is better than nothing
    - Open APIs are a great plus

Privacy

- "Their" Privacy
  - Your data represents an implicit trust relationship with your network – breaches violate that trust
    - Donors, supporters, allies, staff, etc
  - Have a privacy policy for all types of data
    - Follow it. Really.
    - Always consider physical security issues
  - Know the privacy policy for your hosted data
    - Where is it physically stored, under what jurisdiction?
    - Think triple-hard about whether to put sensitive data on corporate servers

Privacy

- "Your" privacy
  - Assert your expectation of privacy in all matters
    - Use secure communications, especially over wireless
    - Encrypt sensitive data (even remotely if possible)
  - Some hosted services are presumed to implicitly waive your expectation of privacy
    - GMail
  - Consider the implications of your non-private data practices

Summary - The 5 Concepts

- Unity
  - Know your data universe and treat it as such
- Redundancy
  - Have a complete and sustainable backup process
- Control
  - Take the steps to avoid losing access
- Portability
  - Confirm your migration options in advance
- Privacy
  - Honor “theirs”, assert “yours”