Data Loss and Recovery

Strategies for Organizational Change

Jill Sexton, Associate Director for Digital & Organizational Strategy, NC State University Libraries

Bradley Daigle, Executive Director, APTrust

CNI Member Meeting
Washington, DC - 13 December 2022
Digital Preservation and Organizational Responsibility

- **Strategic Framework**
  - Key roles identified
  - Policies in place (and updated)
  - Shared responsibility
  - Requirements defined and understood

- **Digital preservation is ACTIVE**
  - Resist organizational inertia

- **Digital preservation is about assurance**

- **Practice data loss scenarios**
  - Fire drills
APTrust Quick-take

- Consortia dedicated to addressing the challenges of digital preservation
- 19 Members, high level engagement
- Incubated in 2011
- Dedicated to transparency - all documentation is publicly available
NC State University Libraries Background

In 2019 the Libraries completed an in-depth evaluation of digital preservation storage infrastructure. Factors at play:

- Shakeup in the digital preservation environment (collapse of DPN)
- Examination of our investment portfolio. Why pay for platforms we are not using?
- Increased affordability of cloud storage solutions
- Frank assessment of our staffing levels and expertise, and a desire to set the Libraries up for a more sustainable future
NC State University Libraries Background

In 2019, the Libraries had about 60 TB of data, with anticipated growth of 10TB year. We sought to safeguard against the following risks:

- Hardware failure and decay
- Environmental threats, e.g., natural disasters
- Organizational change
- Multi-year budget freeze
- Malware/ransomware attack
- Accidental or malicious action by staff

We selected APTrust as our digital preservation platform and began uploading content immediately.
When disaster strikes...

In June 2021, an accidental action by staff resulted in deletion of a ~35TB locally hosted special collections storage volume and its backup.

After review, all but 16 TB were able to be restored from local datastores. This is what we needed to restore from APTrust.

Took about 6 weeks to complete the restore process.

Root cause: incomplete documentation, distributed institutional knowledge, lack of visibility into dependencies, inadequate change management controls.
What went well

Successful data recovery
Costs contained
Effective communication
Great teamwork

A thorough After Action Review resulted in a list of actions to undertake to help prevent future incidents.
What could have gone better

Local storage recovery methods, policies, and roles did not exist before the incident.

It’s important to test, practice, and define those roles before an incident occurs.
When disaster strikes

The APTrust perspective

● The major considerations
  ○ Cost
  ○ Time
  ○ Success

● Security audit and post-mortem
NC State: Lessons Learned

Accurate documentation

Real-time dependency identification

Enhanced change management procedures

Intentional knowledge sharing

Assessment of our strengths and our capacity, which have informed an evolution of our infrastructure to make it more stable and sustainable in the coming years.
NC State Team

Kevin Beswick
Jamie Bradway
Chris Bowen
Brian Dietz
Mike Kastellec
Jason Ronallo
Trevor Thornton
Data Loss and Recovery

Thank you!

Jill Sexton - jksexton@ncsu.edu

Bradley Daigle - bradley@aptrust.org