Digital Library Disaster Planning

Bryan Hamilton

IUPUI

Digital Libraries

Dr. Lamb

4/11/2016
Digital Library Disaster Planning

Introduction

Like everyone out there, libraries face possible disasters every day. LeFergy (2012) mentions three types of disasters that can affect libraries – natural, infrastructure failure, or human action or error. Altman et. al. (2009) list four types of threats to assess when planning for disasters: Physical, Technical, Human, and Institutional. Physical threats are natural or age related (Altman et. al., 2009). This also includes failures of technology. Technological threats are software and format related (Altman et. al., 2009). This includes viruses and outdated formats. Human threats are curator errors and attacks from people within and outside of an organization (Altman et. al., 2009). Institutional threats deal with changes in the mission, legal aspects, or the economy (Altman et. al., 2009). In some cases, the damage might not even be that visible, like bit rot, which needs special tools to locate and stop it (LeFurgy, 2012).

A disaster plan is a document describes the “policies and procedures” “created to prevent, prepare for, respond to, and recover from a disaster” (Muir & Shenton, 2002). The first parts of disaster planning are preparedness and prevention (DeCandido, 1999). Preparedness is “being ready to handle disasters and emergencies”, which includes “risk assessments, disaster planning, adequate supplies, trained staff, and community partnerships” (FEMA, 2005). Disaster response and data recovery are also extremely important parts of a library’s preservation program (Frank & Yakel, 2013). Response is “the actions taken to deal with a disaster or emergency” (FEMA, 2005). Recovery is “restoring services, facilities, programs, collections, and infrastructure (FEMA, 2005). These four parts make up a disaster plan – Preparedness, Prevention, Response, and recovery.
Frank & Yakel (2013) mention two approaches to digital preservation that are used today. The first is LOCKSS, which stands for Lots of Copies Keeps Stuff Safe. The second approach using Integrated Rule Oriented Data System. This system was not originally designed for digital preservation, but helps manage information over large areas and associated with many domains (Frank & Yakel, 2013).

Digital disasters may not happen often, but the damage that does occur is usually not small (LeFurgy, 2012). Disaster planning will not always be able to save everything, but it can lessen the damage and the costs (DeCandido, 1999). Mitigation is “the process of preventing or minimizing” loss and damage from a disaster (FEMA, 2005). When digital data is being stored, librarians must think about the steps needed to prevent the loss of that data or, because that is not always possible, steps to minimize that loss (LeFurgy, 2012).

When a disaster occurs, the most important thing to consider is the safety of the staff and patrons, then think about retrieving collections and restarting services (DeCandido, 1999). There are some steps that have been used in setting up a plan. Someone should be in charge of disaster planning (DeCandido, 1999). A notebook should be created containing important information, like disaster recovery services, insurance information, and vendor support (DeCandido, 1999). One copy of this notebook should be kept at the library and another copy should be kept off site, but accessible (DeCandido, 1999).

A library’s regular routines are essential to creating a digital disaster plan (DeCandido, 1999). When these practices become routine, they will continually be done and they will be done right. A library should do scheduled periodic backups of library data using tapes or discs and these should be kept at a different location and these backups should become a natural part of the daily or weekly workflow (DeCandido, 1999). Staff should also be trained to back up the
important data on each of their work computers, because losing this information might be even more shattering than losing library statistics or other similar library information (DeCandido, 1999). If the backups are done at scheduled and regular times, like daily or weekly, they will become a regular and routine part of the operations and it will not be a problem later if something happens.

Regular maintenance of library technology, like computers and other hardware, is an important part of disaster prevention (DeCandido, 1999). Keeping technology in great working order will help to prevent issues with that equipment later similar to the upkeep of an automobile.

System vendors can’t always recover lost data, which would require a data recovery service (DeCandido, 1999). System vendors’ responsibilities should be clearly outlined in their contracts (DeCandido, 1999). This will make sure the library knows if the system vendors will help if there was ever a need to recovery data. Some staff are able to recover lost data, but because this is a tricky undertaking and professionals might need to be called in to ensure that the process goes smoothly (DeCandido, 1999).

Challenges

There are two challenges associated with digital library disaster planning. One deals with the lack of clarity of the practices for digital library disaster planning. The other deals with the time required and the difficulty of the planning.

Even though digital preservationists have been working on “awareness and understanding”, no set practices are in place for digital disaster preparedness (Frank & Yakel, 2013). ISO 16363 and ISO 14721 standards have helped clarify best practices for disaster
response and recovery of digital information, but two things are still hazy - what are disaster planning activities and what are best practices? (Frank & Yakel, 2013).

Disaster planning is very time consuming and is an extremely difficult activity for librarians (DeCandido, 1999). Many times, disaster planning is put off because of the time commitment and because people do not see a return right away (DeCandido, 1999).

Past, Present, and Future

Disaster planning started in the analog era, but became essential in the digital era (Aikin, 2007). 2007 marked the year when more digital information was being created than could be stored (Bergman, 2008). This required people to focus on not only how to preserve digital information, but also on what information to preserve (Frank & Yakel, 2013). This created problems for librarians – what should be preserved and what should not? Digital curation deals with giving value to digital collections over their lifecycles, including the processes used to create the information contained in them (Frank & Yakel, 2013).

Many people think that digitization is a way to access data and deliver it to others (Palmer, 2014). Some now think that it can be a tool in digital disaster preparedness Palmer, 2014). Palmer (2014) was a little skeptical when she first heard about digitization as a tool for preservation. That is not how she knew of digitization, but things are changing. Information is changing. Data is changing. Technology is changing and improving. New ways of doing things need to be created. Digitization can allow for replication (multiple copies) and redundant backups, which is possible with plentiful storage (Palmer, 2014). Policies and procedures for digitizing materials can be used as a blueprint for the retrieval of collection data (Palmer, 2014). When digitizing information, it is extremely important to write down “unique identifiers and file
format naming protocols” so staff know what to use and are not confused (Palmer, 2014). This information will also make the process more uniform.

Because there is still some haziness on what activities need to be performed and what the best practices are, there is some work that needs to be done. Advocates will continue to work on these best practices. New technologies will be created to present and store data and to preserve and recover that data.

Examples

Avant-Garde 3:AM Magazine used an outside service to manage their servers. One day, they tried to access information saved on those servers and were denied access. They thought at first that there was a technology issue, but their servers had been shut down by the service providers and the company could not get in contact with them (LeFurgy, 2012).

Employees at Pixar were working on Tot Story 2. Data was contained in many different connected files. Data in those files started disappearing. They retrieved back up files of the data only to find out that data was corrupted. They had to pull up different versions and piece together enough good data to fix the problem (LeFurgy, 2012).

On July 3, 2002, a fire destroyed server room/ office at Western University’s College of Business Administration. Smoke from the fire also caused a lot of damage. Damage to the servers was extensive. The College did have tape backups, but the data was very fragmented. They contracted out to Belfour International after the incident to help with recovery and repair of the smoke damaged systems. Their assessment of the situation was that none of the computer systems or components in the server room were deemed recoverable, but all of the other computers in the building, which housed individual employees’ information was salvageable.
This was a great benefit to the College and the staff, because that information was created by various people and just housed on specific computers (Ross et. al., 2005).

This example shows Penn State University’s Disaster Response and Recovery Planning page. The page includes a Disaster Plan Manual template link and a link to information about the 1993 Pattee Library Water Emergency.
This example shows Harvard Library’s Disaster Preparedness page, which includes information on plans, trainings, supplies and a bibliography.
This example shows the University of Michigan Library’s Emergency Response page, which includes links to a Disaster Response and Recovery Plan and a brochure on how to salvage wet books.
References


http://go.galegroup.com.proxy.harrison.edu:2048/ps/retrieve.do?sort=RELEVANCE&docType=Article&tabId=T002&prodId=AONE&searchId=R1&resultListType=RESULT_LIST&searchType=AdvancedSearchForm&contentSegment=&currentPosition=1&searchResultsType=SingleTab&inPS=true&userGroupName=indi8729&docId=GALE|A16424241&contentSet=GALE|A164424241&authCount=1&u=indi8729
