Risk Management and Disaster Recovery Planning for Online Libraries

Ray Uzwyshyn, Ph.D. MLIS MBA

Figure 1 Online Library Homepage

Introduction

Disaster recovery is an important practical risk management area for online IT systems. It is especially important for universities and academic institutions with online libraries where system integrity is dependent on 24/7 continuity for students, faculty and the university infrastructure. Academic Libraries in the 21st century are increasingly electronic with both massive e-book and e-journal holdings and the associated systems which accompany these holdings. This paper discusses pragmatic work experience, observations and current research on disaster recovery mechanisms for online libraries.

It focuses particularly on disaster recovery and risk management strategies for online academic and special libraries. By ensuring disaster recovery, an online library helps ensures the viability of the university system if a natural and man-made disaster befalls the associated physical university or the associated online learning management system (LMS) goes down.

Currently, the general status of online library contingency planning is unsatisfactory or poor. Hurricanes, floods, university closures caused by inclement weather or other threats occur increasingly frequently. If any thought has been given in the past to library disaster recovery planning, this has largely been to the physical library and contingencies based on paper and print collections. Many guidelines too frequently focus upon fire-centered sprinkler system/emergency procedures written to protect physical holdings and staff. While extremely important, there are now major parts of libraries online. With most libraries shift even more to online modalities and content collections and services, times have changed. Lack of widespread emergency planning is not strictly because of neglect but rather budgetary priorities and for the most part, across the board strapped library budgets. The problem is significantly widespread enough that most online libraries plans even if they do exist are reactive or years out of date rather than proactive and current. In this light, the following wider admonitions and prescriptions are forwarded as both pragmatic plan and opening sets of considerations.

Online Libraries, Distributed Systems – System Overview

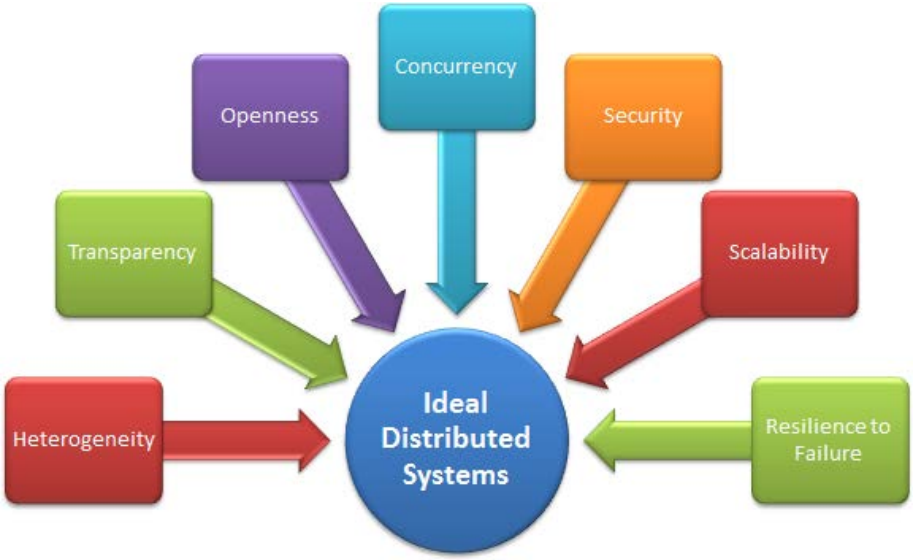

Figure 2: Challenges to Online Libraries as Cloud Based Distributed Systems

Online academic libraries are essentially large and complex distributed information systems. These systems consist of a number of a separate smaller information systems threaded together to create a large synthetic whole. The integrated system will usually comprise a central web infrastructure, either homegrown or managed content management system (CMS), an integrated library online catalog (ILS), connections to multiple specialized subject article, e-journal and e-book databases (at times hundreds) and several information discovery tools that aid in seamlessly tying systems together and providing the end user with a relatively transparent research discovery and retrieval experience.

For a university or academic institution, the online library system also connects to several university systems, most importantly, the university online/learning management

system (LMS) and various security/firewall systems, chief among these being the library proxy server.

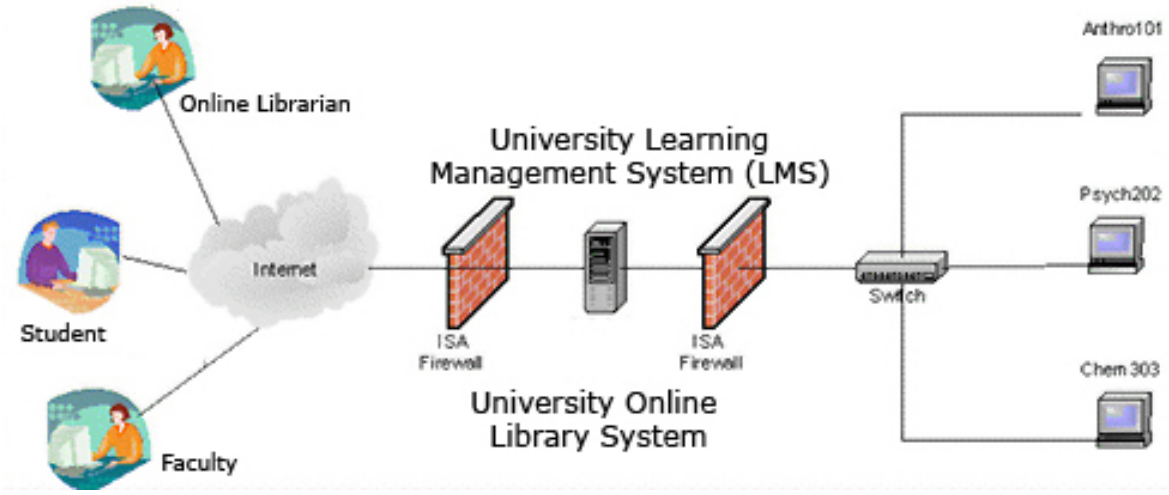

Figure 3: University Learning Management Systems

Disaster Recovery & Distributed Online Library Systems

Crisis Response Sheets

For the most part, the majority of a library's information systems reside in the cloud with the exception of the library's web infrastructure. Most library content (e-books, article databases) physically reside on servers located on external content providers from locales ranging from Palo Alto and Silicon Valley to New Jersey to England, Europe and even Australia. Because of the system's globally distributed nature, it is important to keep a crisis response sheet.

Product	Web Page	Support
ABC Clio US at War Greenwood Press, Praeger Security Int'l	Link	techsupport@abc-clio.com
ACLS Humanities E-Book	http://ezproxy.apus.edu/login?url=http://www.humanitiesebook.org	
Alexander Street Press-VAST video Pkg	http://ezproxy.apus.edu/login?url=http://ahiv.alexanderstreet.com	support@alexanderstreet.com
AquaBrowser	http://ezproxy.apus.edu/login?url=http://apus.aquabrowser.com	clients@serialssolutions.com "if you experience a down system, please make sure to select 'site down' as the category in the support form. This will automatically email all AquaBrowser support staff and ensure you get the fastest response."
Auto Graphics (APUS Catalog)	Link	helpdesk@auto-graphics.com

Figure 2: Crisis Response Sheet Example: Database Services[1]

A crisis response sheet typically consists of outside database content providers and contact information to technical help. For example, the American Public University System library "crisis response" manual is currently much longer than a sheet and presently consists of approximately 20 pages of procedures. It is wise to designate staff personnel to keep this manual current and updated. Kadlec usefully prescribes several general IT disaster recovery procedures that online libraries would do well to implement.[2] These include: providing employee training, predetermining backup offsite storage and recovery procedures and selecting IT methods of notification and continuity. [2]

Most library offsite content providers possess mirror sites and backup links should their initial system servers experience downtime. Rapport needs to be proactively established with technological human resource personnel at each external database

vendor to plan for system contingencies. Mearian further suggests surveying one's cloud service providers to make sure geographically dispersed hosting facilities are in place.[3] Internal personnel and staff will need to be kept informed with regards to procedures in case various database problems are reported. This is particularly important for an university where operations are virtually 24 hours/day and 7 days/week with expectations for a higher caliber of services.

A risk management plan should also include at the least documenting methods, staff roles and responsibilities and contingency budgets. Documenting methods should include a formal set of plans that all staff are aware of depending on the size of the onine library. This also should be developed in tandem with IT (university or corporate), staff and external stakeholders. Any changes to the system should also include updating the disaster recovery plans for the constant changes that typically take place in an online library over a yearly basis. All staff should be aware of their roles within disaster scenarios and these should also be formalized within the plan. Finally, a contingency budget should be developed to either fund immediately with regards to disaster needs or for a system head or director to have at the ready should the opportunity arise for funding. Some of these areas are developed further in the remainder of this research.

Common costs for contingencies include backup servers, offsite storage facilities backup media arrays hard drives and backup personnel support time required for this area. Online library emergency planning budgets will widely range depending on the size of the library. For a small online library, this may be a recurring budget of 12k/year divided into: backup server (3k), backup hard drive array (3k), backup media (2k), 4k,

personnel time costs. This can easily scale for mid-sized operations to 50k and upwards with a wider set of backup server redundancy and disk array backup. 100k-250k annually for large academic library online operations are not uncommon where one or two dedicated personnel positions are needed to maintain consistency in backup and maintain the backup system.

Content Management Systems and Web Infrastructure Disaster Recovery

An online library's main web infrastructure or content management system should reside on its own internal servers. In terms of risk management and disaster recovery, this is preferable to partnering with the associated online university IT infrastructure. If a disaster case should occur and the university server structure experiences disruption, the online library system will be spared. This is especially important for large online library systems where the complexity of the system needs to be protected. Beyond separation from the main university systems, an offsite mirror and archival image of the web infrastructure should be implemented preferably far away from the main library server locations (at least 500 miles). This distant location ensures that if a local storm, hurricane or tornado occurs, a backup server image is simply a phone call away. Staff procedures should also be implemented ahead of time to account for these eventualities.

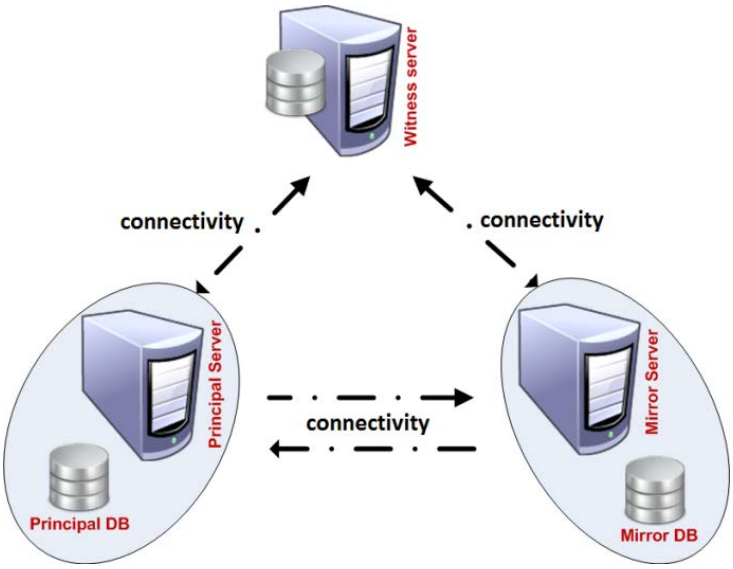

Figure 3: Online Library Mirror Servers[4]

A backup mirror server is a valuable tool for the far more frequent occurrence of server crashes. The larger idea with the library online web infrastructure is that frequent backups should be made on daily, weekly and monthly basis especially with more active changing web infrastructures. In terms of risk management, it is also a good idea for the IT project manager to periodically test these mirror backups and do spot checks. This way there will be few surprises when an actual disaster occurs. With mission critical web infrastructures, the best policy should be trust but verify. If there are online library archives for graduate theses or digital content, multiple copies in separate locations should be kept. Marshall Breeding and others suggest the industry best practice of making use of Stanford university's Open Source LOCKSS Tool (Lots of Copies Keep Stuff Safe, http://locksss.stanford.edu) as any digital library archives expand.[5]

Risk Management – Wider Perspectives

While much of the risk management discussed above involves the incursion of additional financial expense in terms of hardware, software and human resources, negative risk management is really a form of insurance. In terms of an online university, the integrity of the online library ensures both continuity for student assignments, faculty research and the orderly system functioning.

Proactive Disaster Recovery – Risk Management

Schwalbe also usefully presents a spectrum of excellent proactive secondary ideas which may be implemented.[6] Among them:

1) I**dentify System Risks**. In terms of online libraries this means breaking down the complex subsystems that make up an online library system and determining risk factors, interconnectivity with other systems and contingency procedures.
2) **Perform a quantitative risk analysis of the entire system** if such an analysis has not been made.
3) **Plan for various disaster recovery risk responses.** For an online library system this means planning responses from minor and daily/weekly system disruption to complete system meltdown procedures. As systems become complex, documenting these procedures out into a 1 and 2 page highlights and longer manuals for staff is a good idea.[6]

To give a brief example of a quantitative risk analysis for a general online library system it is useful to start with a checklist.

Quantitative Risk Analysis Quick Checklist

Online Library Quick Risk Analysis Checklist	Yes	No
1) Does the library possess one or more backup servers?		
2) Does the online library possess a written online emergency plan?		
3) Is the library in an geographic area relatively free from floods, hurricanes, tornadoes, forest fires etc.? (No such activity in the past 25 years?)		
4) Does the university or corporation of which the library is a part possess a backup or emergency management plan?		
5) Does the library possess an offsite facility for its IT or online infrastructure?		

If the answer to two or more of these questions is no, the library should seriously consider a disaster recovery plan. If the answers to four or more of the questions in the quantitative risk analysis checklist is no, a disaster recovery plan needs to be a very high priority for the online library. Finally, if the checklist reveals a 5/5 assessment, a plan should be carried out immediately as the online library is in fact operating without a safety net.

Monitoring and controlling system risk is always a good idea. By statistically monitoring identified system risks, a project manager gains excellent ideas as to weak system links to be able to proactively plan further. For example, a weak link is always internally controlled servers. While outsourcing or mirror server provisions should be made, this contingency redundancy expense does not always become reality at many institutions where budgets are a factor or wide disaster planning has not reached any critical mass. The important thing for a project manager is to have these contingency plans in place. Proactive readiness is key. At the least, upper management should know these possibilities have been thought about with associated contingency plans so that these can be quickly made should this become possible.

Planning for Long Term Disasters – Physical Analogue Planning

Because an online library is a networked distributed system, if a physical disaster were to occur, the system may be operated remotely from various physical locations. It is important to draw out these contingencies. While no one ever expects a hurricane, tornado or flood to devastate an area, these physical catastrophes do happen. Trained IT staff especially can work wherever a computer and reliable internet connection are present. From IT project management and disaster recovery perspectives, prescriptions are to have this type of plan in place and all staff aware of key point people for this eventuality.

Conclusions

Disaster recovering in an important part of any IT project, especially when projects encompass larger systems and involve institutional integrity. Disaster recovery plans will save a library, university or college time and money. The benefits will repay themselves in manifold manner. Good current literature and further resources regarding disaster planning for online libraries is beginning to appear though for the most part this is online and interspersed with institutional physical recovery scenario planning.[7,8,9] If the physical library or information center becomes inaccessible, an online system can be accessed and worked on from anywhere and by anyone in the academic community. For an online library that is a central and integral part of any university in the 21st century, disaster plans and procedures are imperatives from which the entire university and community will benefit.

References

1. American Public University System. Online Libraries Crisis Response Sheet. APUS Libraries. (2013) Internal Work Document.
2. Kadlec, C.. Best Practices in IT Disaster Recovery Planning. Journal of Internet Banking and Commerce 2010;15:1:1-11.
3. Mearian L.. Disaster recovery gets new urgency. Computerworld. 2012; 46:13.
4. SQLServerHints. Database mirroring in SQL server. SQL Server. Retrieved from: http://sqlserverhints.blogspot.com/2011/06/database-mirroring-in-sql-server-2008.html Accessed March 2013.
5. Breeding, M. Ensuring our digital future. Information Today. November, 2010; 32:34.
6. Schwalbe, K.. Information technology project management (6th ed.). Boston, MA: Cengage. 2011; 244-248.
7. ALA (2013). Disaster preparedness and recovery. American Library Association. Retrieved from: http://www.ala.org/advocacy/govinfo/disasterpreparedness
8. Kroski, E. (2012). Disaster planning for libraries. Open Education Database. Retrieved from: http://oedb.org/ilibrarian/disaster-planning-for-libraries/.
9. SCRLC (2012). Disaster planning and recovery for libraries. South Central Regional Library Council. Retrieved from: http://scrlc.libguides.com/content.php?pid=257029&sid=2147845