JEM

Risk management and disaster recovery planning for online libraries

Ray Uzwyshyn, PhD, MLIS, MBA

ABSTRACT

This article presents an overview of risk management and disaster recovery planning for online libraries. It is suitable for a broad audience interested in online libraries and research centers in universities and colleges. It outlines risk mitigation strategies, and disaster recover planning for online resource-centered information systems.

Key words: online libraries, disaster recovery, risk management, digital libraries, online information centers, information systems

INTRODUCTION

Disaster recovery is an important practical risk management area for online Information Technology (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 twenty-first century are increasingly electronic with both massive e-book and e-journal holdings and the associated systems which accompany these holdings. This article 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 or human-caused 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, and 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 on 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 shifting to online modalities, e-content collections and e-services, times have changed. Lack of widespread emergency planning is not strictly because of neglect but rather budgetary priorities, and for the most part, strapped library budgets. The problem is significantly widespread enough that online libraries plans, even if they do exist, are reactive or out-of-date rather than proactive and current. In this light, the following wider admonitions and prescriptions are forwarded as pragmatic plans and opening sets of considerations.

ONLINE LIBRARIES & DISTRIBUTED SYSTEMS: SYSTEM OVERVIEW

Online academic libraries are essentially large and complex distributed information systems (Figure 1). 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, 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

DOI:10.5055/jem.2015.0264

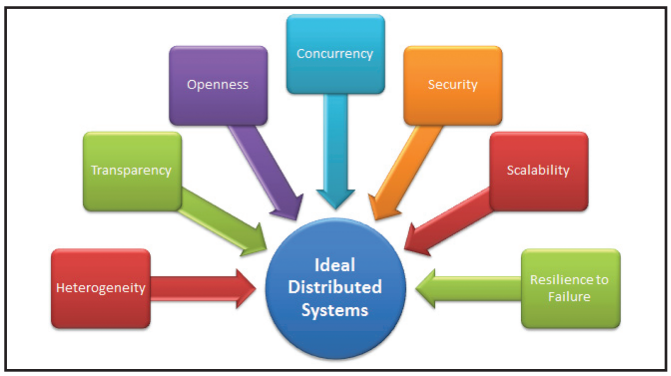

Figure 1. Challenges to online libraries as cloud based distributed systems.

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/LMS and various security/firewall systems, chief among these being the library proxy server (Figure 2).

DISASTER RECOVERY & DISTRIBUTED ONLINE LIBRARY SYSTEMS

Crisis response sheets

For the most part, the majority of a library's information resources reside in the cloud with the exception of the library's web infrastructure. Most library content (e-books, article databases) physically resides 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 (Figure 3).

A crisis response sheet typically consists of outside database content providers and contact information to technical help. Crisis response manuals currently range from a couple of pages for smaller systems to 20-50 pages of procedures for very large systems with many interlocking parts. 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 regarding procedures in case various database problems are reported. This is particularly

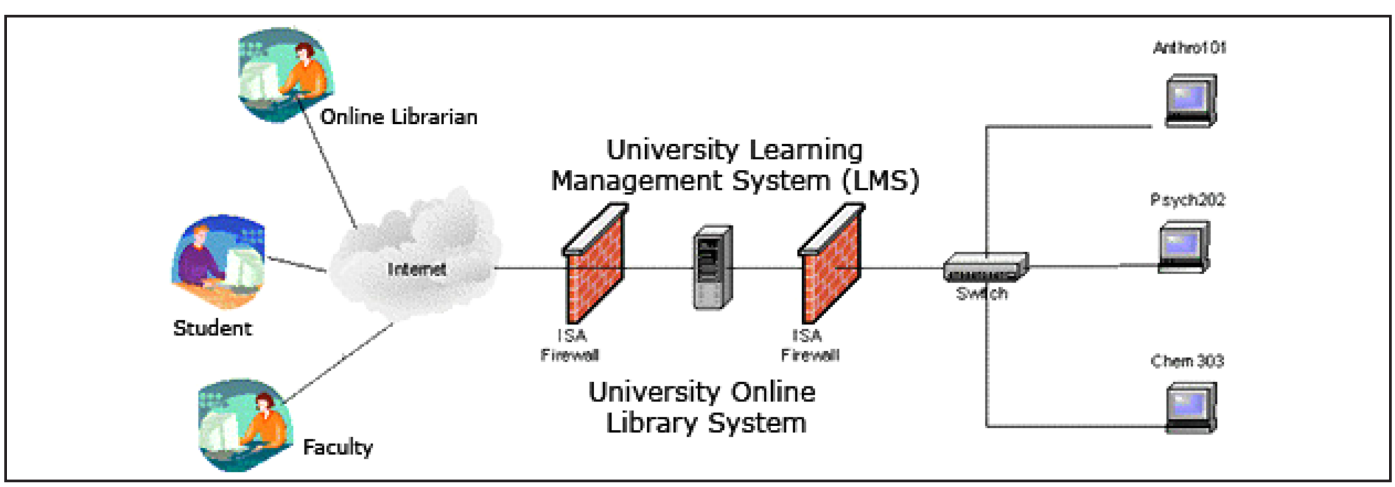

Figure 2. University online library & learning management systems.

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 e-mail all AquaBrowser support staff and ensure you get the fastest response."
Auto Graphics (APUS Catalog)	*Link*	*helpdesk@auto-graphics.com*

Figure 3. Crisis response sheet.

important for a university where operations are virtually 24 hours per day and 7 days per week with expectations for a higher caliber of services.

A risk management plan should also include 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 online library. This should be developed in tandem with IT (university or corporate), staff, and external stakeholders. Any changes to the system should 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 regarding 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 per year divided into backup server (3k), backup hard drive array (3k), backup media (2k) and 4TB tape drive (4k). Personnel time costs can easily scale for mid-sized operations to 50k and upward with a wider set of backup server redundancy and disk array backup. Dedicated IT personnel allocation for large academic library online operations is also not uncommon where one or two dedicated personnel positions are needed to maintain consistency in backup and to maintain various systems and long-term storage and disaster recovery mechanisms.

CONTENT MANAGEMENT SYSTEMS AND WEB INFRASTRUCTURE DISASTER RECOVERY

An online library or research center's main web infrastructure or CMS should reside on its own internal servers. In terms of risk management and disaster recovery, this is preferable to partnering with the associated university or corporate IT infrastructure. If a disaster case should occur and the main 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 100 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 4).

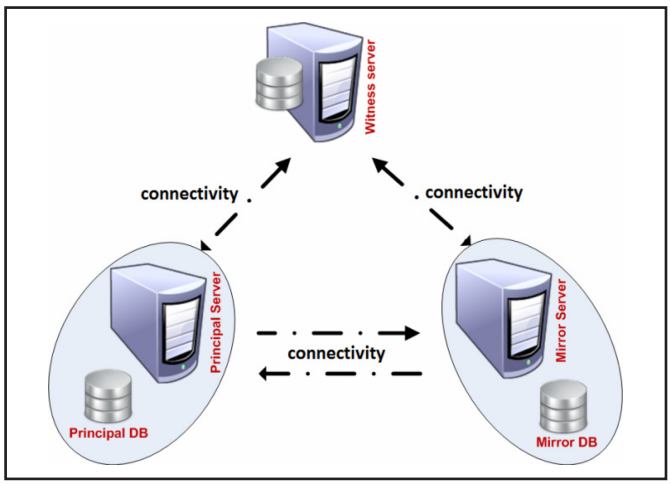

Figure 4. Online library mirror servers.[4]

A backup mirror server is a valuable tool for the 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 a 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] Commercial long-term online storage with facilities such as Amazon's Glacier, S3 or academic possibilities such as DuraCloud, DPN, or UC San Diego's Chronopolis may also be pursued.

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, risk management is really a form of insurance. In terms of an online or physical university, the integrity of the online library ensures both continuity for student assignments, faculty research and the orderly system functioning.

RISK MANAGEMENT

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

1. *Identify system risks*: In terms of online libraries, this means breaking down the complex subsystems that make up an online library 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 into 1-2 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 a 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 high priority. If the checklist reveals a 5/5 assessment, a plan should be performed immediately as the online library is operating without a safety net.

Monitoring and controlling 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 single-point 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 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, management should know these possibilities have been reflected on with associated plans so that these can be made when this becomes feasible.

PLANNING FOR LONG-TERM DISASTERS

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 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 all possibilities.

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 research center time and money. The benefits will repay themselves. Good current literature and further resources regarding disaster planning for online libraries is beginning to appear.[7-9] For the most part this is still largely oriented toward physical recovery scenario planning. 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 or research community. An online library is a central and integral part of any university in the twenty-first century. Disaster plans and procedures are imperatives from which the entire university and community will benefit.

Ray Uzwyshyn, PhD, MLIS, MBA, Director, Collections and Digital Services, Texas State University Libraries, San Marcos, Texas.

REFERENCES

1. American Public University System: *Online Libraries Crisis Response Sheet*. Charles Town, WV: APUS Libraries, 2013.
2. Kadlec C: Best practices in IT disaster recovery planning. *J Internet Bank 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. Available at *http://sqlserverhints.blogspot.com/2011/06/database-mirroring-in-sql-server-2008.html*. Accessed March 2013.
5. Breeding M: Ensuring our digital future. *Info Today*. 2010; 32: 34.
6. Schwalbe K: *Information Technology Project Management*. 6th ed. Boston, MA: Cengage, 2011: 244-248.
7. ALA: *Disaster Preparedness and Recovery*. Chicago: American Library Association, 2013. Available at *http://www.ala.org/advocacy/govinfo/disasterpreparedness*. Accessed February 2015.
8. Robertson G: *Disaster Planning for Libraries: Process and Guidelines.* New York: Chandos, 2014.
9. SCRLC: *Disaster Planning and Recovery for Libraries*. Ithaca: South Central Regional Library Council, 2012. Available at *http://scrlc.libguides.com/content.php?pid=257029&sid=2147845*. Accessed February 2015.