Disaster recovery planning

Introduction

Losing your library data is a frustrating, expensive and unnecessary experience; don't let it happen to you.

This document doesn't pretend to teach you everything that you need to know about disaster recovery, but it should get you thinking along the right lines. Many City and Shire Councils and some schools will already have disaster recovery plans; this document focuses on the elements of such a plan that relate to library management systems.

O'Toole's commentary on Murphy's law – "Murphy was an optimist"

There are a number of events that can bring your library management system to a complete halt, some are temporary, some are not.

1. Equipment failure
   ◦ Hard disk crash
   ◦ Network failure
   ◦ Virus attack

2. Power outage
   ◦ Anything between a momentary disk-frying surge and a couple of candle-lit days

3. Operator/Administrator error
   ◦ Accidental deletion of files or data
   ◦ Mistakes while editing configuration files (INI files)
   ◦ Removal of user permissions

4. Fire
   ◦ The most compelling reason for keeping off-site backups
   ◦ Even if the whole building and collection is lost you will want to recover the data for your insurance claim

5. Theft

These things happen to school and community libraries regularly, if you don't have a good disaster recovery plan you will lose all your data, thousands of catalogue and holdings records, all your circulation information and any value added cataloguing that you have done. You will not be happy.
Make a plan

There are three phases to a disaster recovery plan.

Before

• Preventative

  Are there any actions you can take that might prevent the disaster from happening?
  
  ◦ Replace aging hardware before it fails
  ◦ Use power line filters and/or surge protectors, at least on the server
  ◦ Keep your Operating System up-to-date by installing Service Packs
  ◦ Use up-to-date virus protection software
  ◦ Use only commonly available backup media, software and drives
  ◦ Monitor the amount of free disk space on your database server to ensure that there is enough space for the backups and database growth
  ◦ Follow the OCLC recommended procedures for backups
  ◦ Document the backup and recovery procedures
    • Make sure that each action is assigned to a person

• Preparedness

  Are there any actions you can take that will ensure that you are properly prepared to respond to and recover from the disaster?
  
  ◦ Maintain and check backup procedures
    • If the databases are backed up to disk, SQL Base always does, you also need a process to copy the backup files to some other location and or media for off-site backup
    • Copy the following folders onto the backup media as well as the database backups:
      • Folder containing Images linked to Catalogues
      • Folder containing Images linked to Borrowers
      • Folder containing NetOpac html files
      • Folders containing AmlibNet html files
    • Label backup media clearly
    • Rotate backup media so that you are not over-writing the most recent backup
  ◦ Keep off-site backups of the backup data and recovery software
  ◦ Check the backup logs – allow access for both Library and IT staff for this purpose
  ◦ Keep your Amlib installation CDs – they always contain everything you need to carry out a fresh installation of the client software and also the latest SQL Base Database Management System
  ◦ Carry out a test recovery on to a set of the test databases at regular intervals
  ◦ Install and test Offline on more than one PC etc.
During

• Response

What action should be taken when a disaster occurs?

◦ Use Offline for circulation during power outages and network or server failures.
◦ Power down machines running on UPS devices before the battery fails.

After

• Recovery

What action must be taken to restore library services to normal or at least make data available for the insurance claim?

◦ Borrow, rent or buy a replacement server as soon as possible
◦ Install the required Operating System, Database Management Software and backup utilities.
◦ Restore the Amlib databases from the most recent backup
◦ Install the Amlib Client software from the Amlib Installation CD
◦ Make sure that the new system is working

Allocate responsibility

Decide who is responsible for each action that is specified in the plan and make sure that the person acknowledges the responsibility.

Practice

At regular intervals, practice recovering your library's databases from the most recent backups. This is one good reason for having a set of test databases, you can practice restoring from a backup on them with no risk to your live data.

Put these regular practices into your plan.

Review

Over time software systems change, new utilities get installed, web pages are updated, new people move into important roles; this means that your plan may become out-of-date. To avoid this review you plan at regular intervals.

Staff changes are a big cause of problems in Backup and Recovery procedures. Review the whole process with each new person so that there is a clear understanding of what is being done, why it is being done and by whom.
References