

DISASTER PLANNING FOR COMPUTERS AND NETWORKS

By Richard W. Boss

Libraries are subject to disasters, both natural and manmade. It is essential to plan for them in order to prevent them when possible and to recover from them as quickly as possible when they do occur. This Tech Note is limited to disaster planning for computers and networks, but libraries should undertake disaster planning on a comprehensive basis, with the protection of computers and networks but one component of its disaster plan.

Disaster planning for computers and networks is important because these technologies are essential to patron service and staff productivity. Not only is the patron access catalog the only way for patrons to identify holdings and current availability of titles in their library, but also titles in other libraries and electronic resources to which their library subscribes. For many, their only access to the Internet is through their library. Library staff are dependent on these technologies for ordering, claiming and receiving library materials, charging and discharging of library materials to patrons; and the provision of reference service. Every hour of downtime is extremely serious, therefore, a library must give disaster planning a high priority.

Definition

A disaster is defined as a sudden misfortune that is ruinous to an undertaking. This means that there is little time to react at the time of the misfortune. Preparations have to have been made in advance. The focus should, therefore, be on disaster planning.

Risk Assessment

A computer or network disaster typically involves loss of or damage to data, the inability of programs to function, or the loss of data communication. The first step in disaster planning is to assess risk. What is the probability a particular disaster will occur and how serious is the effect likely to be if it does occur? Among the disasters that should be assessed are natural disasters such as floods, fires, and earthquakes and manmade disasters such as air conditioning failures, viruses, hacking, and vandalism. The line between the two is not clear-cut because a flood can be the result of vandalism to a water pipe and a fire can be deliberately set as an act of vandalism.

A risk assessment matrix should be created, one which puts the probability on one axis and the effect on the other, with the risk factor fixed by the combination of the two factors:

EFFECT Major Moderate Minor High 5 4 3 PROBABILITY Moderate 4 3 2 Low 3 2 1

A risk factor of 5 requires much more attention and warrants a much greater outlay of resources than a risk factor of 1.

The risk factor will vary by area of the country, nature of the community, and type of organization. In much of California, earthquakes would be rated a risk factor of 5; along the flood plains of the Mississippi River flooding would be a risk factor of 5. Viruses, while probable, usually have only a minor effect, therefore, they would have a risk factor of 3. Hacking, which rates highly probably for Fortune 500 companies, rates low for libraries, but may rate a risk factor of 3 because its effect may be major. In many areas floods are likely to be the result of a broken pipe and have a low risk factor of 1 or 2 because their effect tends to be localized and, therefore, minor or moderate.

Risk Reduction

The second step in disaster planning is risk reduction. This is achieved by lowering the risk factor by reducing the probability, reducing the effect, or both. For example, while no disaster plan can reduce the probability of an earthquake, building a library in California that is quake-resistant should reduce the effect of one. Placing a computer room where there are no overhead pipes reduces the probability of flooding; rack-mounting the computer hardware so that it is several inches above the floor reduces the effect. Installing anti-virus software reduces the probability of a disaster; regularly backing up all data reduces the effect.

Needed Resources

Disaster planning takes time and expertise, but it is within the means of most libraries. A small task force of staff members, given time to read the literature and contact other libraries that have done disaster planning, can develop a disaster plan in weeks or months. What is difficult for many libraries is finding the funds to carry out the plan. Retrofitting an old building to withstand earthquakes can cost hundreds-of-thousands or millions of dollars; mirroring a library's database of bibliographic and patron records can cost tens-of-thousands of dollars. Each risk factor must, therefore, have a price tag associated with it. A library has to decide whether the risk reduction is worth the price and, if so, seek the funds to pursue the risk reduction.

It may not be realistic to lower the highest risk factors first because the funds may not be available. It may be necessary to focus on lowering risk factors for which the resources are available. Heat/smoke and water detectors are within the means of most libraries and should not be skipped over just because the risk factor is not a 4 or 5.

Common Disaster Plan Elements

Every disaster plan should set forth both preventive measures and remedies in at least the following areas:

Servers

Every library with one or more servers should have a server room that is secured with a combination lock such as a Simplex and a reinforced door with a deadbolt at least 1.5 inches long. If the room is not windowless, the windows should be barred. The room should have both fire/heat detection and water detection sensors which set off a local alarm and send a signal to an off-premises monitoring facility. At a minimum, it should have fire extinguishers suitable for electrical fires. A library that has hundreds-of-thousands of dollars in equipment in its server room should consider a built-in fire suppression system.

Excess heat is, by far, the most commonly reported cause of server downtime and damage. A library should, therefore, augment its building air conditioning with a room-size air conditioner that kicks-in only when its thermostat shows that the temperature in the room has risen above a library specified level, typically 68 degrees. An additional safeguard is available, a thermostat inside any cabinet which has a cooling fan. When a fan fails and the temperature rises, an alarm should be triggered.

Water damage is the second-ranking cause of server downtime and damage, although the damage is rarely greater than moderate. There should be no water pipes in the ceiling above the room, or in the walls that enclose it. The server(s) and associated peripheral equipment should be rack-mounted so that up to six inches of standing water will not affect the equipment.

Power irregularities are the third-ranking cause of server downtime and damage. An UPS (uninterruptible power supply) should be used to protect all servers against surges, spikes, brownouts, and blackouts. The UPS should have a rating which is at least twice the total KVA requirements of the devices it protects. KVA (Kilo Volt Amperes) is a rating that is calculated by multiplying the number of volts by the number of amperes and dividing by 1,000. While a library may not want to operate its servers on battery back-up for an extended period, the UPS should provide power long enough for an orderly shutdown of all servers.

The database server should be protected by its own firewall, preferably a proxy-server between it and the Web server on which the patron access catalog is mounted. A proxy server shields the database server from direct access by initiating a separate inquiry, rather than passing the external inquiry through to the database server. The firewall can be on the same hardware platform as the database server. The Web server can support not only the patron access catalog, but also other files and a gateway to electronic resources outside the library. It should include remote patron authentication software so that access to other than records the library wishes to make available to everyone is limited to those who are registered library users.

Each server should be configured with a logging tape drive--typically a 4mm or 8mm streaming tape drive-- so that all information written to disk is also written to tape. Each evening the logging tape should be removed and stored away from the server room and a new tape mounted for database back-up. Overnight, the content of the disk drives should be written to tape. The next morning, the back-up tape should be removed and stored away from the server room and a new tape mounted for logging that day's transactions. It will then be possible to restore all files using the most recent back and logging tapes. Magnetic media can become unstable with repeated use, therefore, seven logging tapes--one for each day of the week--should be used. Seven back-up tapes should also be used. All of the tapes should be replaced at least every year.

A library may choose to do a back-up only once a week. If so, all of the logging tapes for the week should be saved so that they and the previous week's back-up tape can be used to restore the files. The logging tapes and the previous week's back-up tape should be stored away from the server room. In a large facility than may be at the opposite end of the building, but for smaller facilities it should be off-site.

At least once per week, a current back-up tape should be sent to an off-site storage facility to protect against the loss of the on-site back-up tape.

Libraries that can afford RAID (Reduced Array of Inexpensive Disks) should configure their servers with them. RAID technology mirrors everything written to one disk on another disk. If a disk fails, the mirroring disk provides access to the information without resorting to the rebuilding of files from the combination of back-up and logging tapes.

The database server for the automated library system should be available only to library staff in the library and the vendor of the automated library system. It should not be available to others via the Internet or by dial-up. Patrons should instead, access the patron access catalog on a Web server.

Network

A library can do a great deal to secure a LAN (local area network), but only a limited amount to secure a WAN (wide area network). The former usually is limited to a single building or part of a building; the latter usually ties two or more LANs together using a telco or other common carrier's circuits. The telco or common carrier has the responsibility for its portion of the WAN.

The preferred LAN topology is a hybrid star, one that has several central star network points linked in a star. In other words, several desktop clients are connected to a hub, and several hubs are connected to yet another hub. The cabling from the desktop clients to the hubs can be relatively inexpensive Category 5 UTP (unshielded twisted pair); the wiring among hubs should be STP (shielded twisted pair) or fiber optic to dramatically improve performance and security.

Network hardware should be secured in locked data communications closets or cabinets. All data jacks should be capable of being de-activated when no library equipment is connected to them. The practice of distributing a large number of data jacks around a building for use by patrons with laptops should be avoided unless these jacks are on a separate LAN segment that can be isolated from the database server of the automated library system. Patrons need access only to the patron access catalog, and possibly to other servers: Web, Internet, CD-ROM, image, etc.

If a wireless LAN is implemented, it should access only a segment of the library's LAN, one that can be isolated from the database server of the automated library system.

The most vulnerable part of a library's network is the connection to the Internet, both access from the Internet to its servers and from its servers and clients to the Internet. Fortunately, it is cost effective to protect a library's database server with its own firewall so that there is protection against in-library users, as well as external users. More vulnerable are the other servers and the clients or desktop workstations. Most libraries seek to protect them only from users outside the library. This can be done by installing a network firewall. The firewall can be configured not only to restrict access to specific categories of users or specific types of queries, but can also be configured to facilitate access to library-selected resources.

Clients

PCS and Macs are the most vulnerable technology in libraries because they can be compromised by staff and patrons who behave unwisely by downloading attachments or bringing in software and data disks from outside the library. Viruses are the greatest threat. Anti-virus software is absolutely essential. Products from companies such as McAfee and Norton detect computer virus signatures and alert the user to them before they enter the client, however, anti-virus products are of little value if they are not regularly updated. Literally hundreds of new viruses are unleashed every week, therefore, anti-virus software should be updated at least weekly by downloading the latest version.

Almost all viruses travel via e-mail attachments or diskettes. Staff should, therefore, be instructed not to open an attachment if the source of the e-mail is not known or the attachment is not expected. They should be particularly suspicious of attachments with strange-sounding titles. When in doubt, the sender should be asked by return e-mail to describe the contents of the attachment. Staff should be instructed not to bring software from home for loading on library machines, nor to carry diskettes back and forth ("sneakernet") between home and work machines.

Recovery Procedures

It is important to state in the disaster plan not only what recovery procedures are to be followed if a disaster occurs, but also who has what responsibility. Who calls whom and what information should they be prepared to give? Who performs the needed diagnostics?

Who restores the files? What are the instructions for packing and shipping the corrupted files?

Communication

Communication is of great importance during a disaster. It should not be assumed that regular telephone service will be available. Key personnel should have cell phones for use when regular telephone service fails or is overloaded. The cell phone in the server room should be stored in a wall-hung watertight cabinet on the wall adjacent to the entrance door. The instructions for dealing with a computer/network disaster should be stored in the same cabinet. All important telephone numbers should be stored in each cell phone. If a disaster affects more than the library, the cellular service may be swamped with calls. It is, therefore, a good idea to instruct the operator in the server room to use the redial and speaker features of the regular telephone while seeking to get through on the cell phone.

Designated operators

There should be a server operator on duty each hour a library is open. This may be a member of the circulation desk's support staff--the staff which usually is in the library all of the hours a library is open. The designated person would perform the end-of-day swap of the logging and back-up tapes as part of his/her routine duties. Otherwise, s/he would leave her/his regular duties only when there was a problem.

The designated operator on duty at the time of a disaster should have instructions to call the support desks for the servers that have been affected. The numbers should be encoded in both the server room's telephone and the cell phone that has been provided as a back-up.

Each designated operator should participate in an occasional disaster drill that simulates an actual disaster that affects one or more servers.

Designated manager

An operator may encounter a situation that overwhelms him/her. There should always be a designated manager in the library or available by telephone 24 hours per day, seven days per week. While there may rarely be a need to decide about evacuation of the library or another major action, the capacity to do so must be in place.

External resources

The vendor of an automated library system is an important resource in diagnosing problems that result from a disaster. When drawing the contract, make it clear that the vendor shall be liable not only for the performance of the central site and its client software, but it shall undertake remote diagnostics through the network to the desktop. In other words, it shall pinpoint a problem regardless of where it is. If coverage has not been

purchased for 24 hours a day and seven days a week, there should be provision for emergency support at agreed upon hourly rates outside the normal coverage hours.

If the database server for the automated library system is affected by a disaster, the vendor's trouble desk should be called so that remote diagnostics can be performed and guidance can be obtained. If the vendor of the automated library system is not responsible for the management of hardware maintenance, hardware problems should be referred to the manufacturer's support desk.

With few exceptions, the vendors of automated library systems operate service bureaus for libraries that do not wish to maintain their own computer systems. A library should discuss the terms for its vendor to offer its service bureau as a back-up facility should the library not be able to restore its own system within a day or so. This will involve establishing a basic profile and maintaining a relatively recent copy of the library's database at the vendor's site. Since access to the server will probably be via the Internet, performance will not be the equal of that possible with a local server.

Sources of support for all other servers should be identified and their telephone numbers encoded in the server room's telephone and in the cell phone that have been provided for back- up.

Most libraries do not have the luxury of a network specialist. A library should, therefore, rely on the networking staff of a parent organization or consider contracting with a network support service for remote diagnostics and recovery assistance. While these firms are found in most major cities, a regional or national firm with experience in automated library systems should be considered.

One or more data recovery firms should be identified. These firms recover data from hard drives, diskettes, or any other storage medium that has been damaged by flood, fire, physical impact, or a virus. Rates range from \$50 to \$100 per hour, and most recoveries require fewer than eight hours. A large national firm usually is able to accommodate a rush order better than a smaller local one. The media can be sent overnight by FedEx or another courier service. It is a good idea to establish an account ahead of time.

A library should determine whether its book jobbers and serials subscription agencies will provide machine-readable records of orders placed with them, how quickly they can be available, and at what cost.

Insurance

Unless it is part of a larger organization that carries disaster insurance or is self-insuring, a library should carry insurance that includes coverage for its servers, network, and clients. In order to make claims, it is essential to have an absolutely current inventory of all hardware and software, including purchase data and price. A copy of this information should be stored at a remote site.

In case of damage that is visible, photographs should be taken promptly after the disaster to substantiate an insurance claim.

Sources of Information

Up-to-date information on computer and network disaster planning can be found on the Internet. Specific Web sites are not being recommended because the information on sites quickly goes out of date. Insofar as possible, consult only sites which date their information or which clearly have current information--for example, sites which refer to current versions of standards. However, one site that has regularly been updated is worth mentioning: Intra Computer Inc.'s site on disasters in computer rooms. It can be found at www.intraocomp.com/.

Disaster planning guidelines do not go out of date as quickly. An excellent source for information is a paper written and by Dr. Jan Lyall, Director, National Preservation Office, National Library of Australia in 1993 and presented at an international conference. It is still available at www.nla.gov.au/nla/staffpaper/lyall1.html/. While the guidelines were developed with the protection of library materials in mind, they are useful in any disaster planning.

June 2002