2

Planning for the Worst

Loss of Computer Operations

In the aftermath of September 11, 2001, the Federal Reserve, the Office of the Comptroller of the Currency, the Securities and Exchange Commission, and the New York State Banking Department met to draw up guidelines for the protection of data and the flow of information and monetary funds between U.S. financial institutions. Their concerns for computer systems were:

- rapid recovery and timely resumption of critical operations following a wide-scale, regional disruption;
- rapid recovery and timely resumption of critical operations following the loss or inaccessibility of staff in at least one major operating location; and
- a high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible.[1]

In just the same way, libraries and archives need to be concerned with restoring access to their information and services for their patrons in a quick, efficient manner.

Keeping Up with the Changes

Software

Let's think about preventing the loss of data. What happens if you lose your data in a major server or network crash and it turns out that there isn't a current backup for the software. In fact, the software that you were using was the newest version of some program, and the computer center can't find that version and must use the previous one. Do you realize that you cannot open current data files with older software versions? You can do the reverse, of course: open old files with new programs. So here is another layer to add to backup routines and prevention programs: *back up the software.*

Of course, this disaster could be man-made if you "borrow" someone else's software, install it onto your computer (which is technically illegal unless it is freeware or shareware), and then your computer crashes and you find the only software you own is the older version. You are out of luck and lose all that time for data creation and access to your files, until you can purchase a new software program.

In the same breath, it is important to keep up with software changes. It isn't essential to purchase every upgrade, but pay attention to the industry. When it says that the new program no longer supports your software version, you have waited too long to upgrade and may have problems reading the old files with new software. Unfortunately the same rule applies to operating systems. If you wait too long to change to the new system, then you will find the data and its associated software won't run properly. In fact, this issue snowballs when you factor in the upgrading of your hardware.

When computers first became affordable, many cultural institutions delayed purchase until the "best" system could be found, only to realize that this was never going to happen. The institutions found that they had to buy into hardware and software, hope they had picked the right equipment and programs, and then get on

the upgrade treadmill. If you don't upgrade your hardware when you upgrade the software, you may find that the technical requirements of the software are greater than your computing power.

To cope with the cycle of purchase and deaccession, some institutions lease equipment so they get automatic upgrades of hardware and software when the vendor comes out with new versions. As long as the costs for these upgrades are built into your budget, this works out quite well. Some institutions have instituted a purchasing cycle for hardware and software of anywhere from two to four years. IT departments probably upgrade more often than any other department, say every eighteen months. Support operations are upgraded maybe every three years. Don't establish a purchasing cycle greater than four years, or the technology and learning curve will be too great for your staff to comfortably absorb.

Operating Systems

What operating system are you using today? When did you make that commitment? What happens if you switch from MS Windows NT to Sun's Linux? How will you know which data is stored in which operating system? It is possible that different departments in your institution use different operating systems. Make certain you document any nonstandard formats, programs, and systems. Your computer services department staff needs to document the changes in operating systems, as does your records manager. This will be important for the future retrieval of or access to long-term digital materials.

Hardware

In the context of preventing loss of data, the protection of hardware should include preventing obsolescence. As software modifications increase computing power, your institution, building, and department may be forced to purchase new computer components. You do not need to replace all the equipment, but you need to make certain the older software and peripheral drivers can run the new configurations of hardware and peripherals. When you deaccession the hardware, make certain the hard drives are clean of data by reformatting the disk, not just deleting the data. Check with your computing services department and ask them to help you with this.

What if your computer system is running old computer software on old computer equipment and you can't afford to upgrade? Then you will need to keep that old equipment running. It will also be necessary to find old components and scavenge for old parts. Think carefully about this issue because it is a very costly decision to stay with obsolete systems. The same holds true of homegrown or proprietary software systems. At some point, you will have to find the money and the expertise to convert to a new system. Doing this during a crisis is not the best use of your organization's time, money, and energy.

What will you do if the system fails; either the hardware or the software, or you have a disaster? Have you thought about where you will find the obsolete equipment and software? This is one of the most important reasons to back up your software, operating system, and data. If you are still running your programs and data in DOS or an older operating system and your system dies, you would be really lucky to find someone who has the right software and can help you restore your system.

Protecting Your Assets

On-Site Storage

It is common practice for individuals to keep backup files on diskettes or CD-ROMs at their desks while they are working on projects. It is a good idea to have additional copies stored somewhere else in case you cannot get access to the building.

Fireproof cabinets are designed for paper documents, and in some cases microfilm and microfiche. Fireproof cabinets are usually rated at 1,500–2,000° F. Magnetic media will begin to melt at 125° F. If this is your only method of storage, then you need to make certain that the fireproof cabinets will keep the temperature stable, and cross your fingers. The same goes for safes; they won't keep the magnetic media from melting. In both cases, the safe and the fireproof

cabinet will not necessarily keep out soot, dust, and other airborne particulate matter. Soot and dust will settle on the surfaces of the magnetic media and then abrade these surfaces, causing loss of data should the medium be played prior to cleaning it.

Access to Backup Data

We have discussed the need to back up data and keep track of both the hardware and software required to read your data. Some questions to consider are:

Where do you store the backups?

How much of the system is on the backup tapes? And how often is it backed up?

Do you store the tapes on top of the computer, in a "fireproof" cabinet in the room (both bad ideas), at home, in a physical data storage vault, in the car, with a vendor, at the bank?

At what point do you send the backups from on-site or local storage to remote storage?

Who can get access to the backups?

Can you load the backups in a remote location or access the data from an alternative computing center?

These are some serious questions to ask yourself, the computer/information technology people in your department or building, and those at the institution. Set up a regular schedule for removing storage media from your desk or computer room to somewhere else. This way when there is a loss of data, the physical storage medium will be retrievable and the data can be remounted onto the network.

The departmental contact person should get together with the building computer disaster-response plan team leader to set up backup and storage schedules. The building contact should coordinate with the institution-wide computer disaster-response team for off-site storage protocols and procedures. These storage decisions should be coordinated with the institution's records manager. Discuss how the backup data fits within record-retention schedules for the institution as a whole.

Off-Site Storage

Just when do you transfer the data off-site? Data should be transferred off-site on a very regular basis. Often organizations will keep the most recent backup in their office or a nearby building, and then ship the backup tapes to the remote storage facility once a week. Thus the most current data, that which has been changed recently, is most vulnerable to loss. What might be better is to store the most recent week's data in another building, at someone's home, or even in the car if it isn't too hot or cold outside.

Then on a very regular basis, you want to send everything to the off-site storage facility. Send your data, software, and operating system software. Anything that you cannot live without should exist as a working copy in the remote storage facility.

You have several options for transferring the data off-site. You can physically take it or have it delivered to your storage facility. Many companies will arrange for daily or weekly pickup. You could send the data to a remote data storage facility via the Web, phone lines, or FTP depending upon how much data you have and where the facility is located. Of course, you also want to send the operating system and software to the remote data storage facility on a regular basis to prevent loss of everything.

Perhaps you have more data than is possible to back up every night. This is the case for large institutions, especially those that are extremely data-dependent. Well, there are some other options. In fact, you don't have to be a large organization to take advantage of a number of remote backup service products. So what are they? Well, there are remote backup services that accept your data via FTP or secured data-stream transfer on a regular basis. These businesses provide a software package that allows you to back up on a preset schedule to the remote location. Remote backup businesses can also describe their service as data vaulting. This industry has been around for at least fifteen years.

Data Storage Service Providers

Data storage services run the gamut from providing storage space for backup data tapes to hard-copy storage. Depending upon their sophistication and scope of services, these businesses may be associated with a disaster response company that can help you reload your data. (See appendix B for a list of companies that provide data storage services, etc.) For the most part, they are just storage companies with environmentally controlled areas for computer files. Some questions to ask when picking a data storage service provider include:

- How quickly can you get access to the backups? If you need the data on a 24/7 basis, it is imperative that they provide services around the clock.
- What are the costs and time frames for delivery?
- Do you have to go there to pick up the tapes?
- Are your data arranged in such a way that the storage company can find your tapes? Can they send the information via secured data line?
- Can the data storage vendor provide a hot site or mobile recovery site if you need it?
- Does the vendor have the hardware to set you up for a "declared" disaster?
- Do you have the insurance coverage for this?
- Can the data storage center find your "remote" or alternative location?

Hot, Cold, and Mobile Recovery Sites

"Hot sites" are facilities that are completely wired together with the hardware that your organization needs to get its information services up and running quickly. Organizations contract with these facilities to provide technical support should a disaster be declared. Hot site staff work with computer systems staff to test their disaster response plans in order to determine how long it will take to reinstall software applications and data. When computer systems crash or are unavailable, then the organization declares a disaster and computer staff head to the hot site. When the World Trade Center was destroyed on September 11, 2001, financial industries immediately declared disasters and their computer staff worked to get the companies' data operational as quickly as possible. Those that used data replication or mirroring had their computer services shunted to remote servers and were active almost immediately. Hot site time is traditionally paid for by the computer rider in your insurance plan, although the contract for the hot site is separate insurance and is paid for by the institution. The duration of stay in the hot site is limited by the size and scope of the disaster and the amount of insurance carried.

"Cold sites" are wired computer rooms without the hardware. These facilities are usually rented when the computer staff needs a long-term facility from which to operate.

Mobile recovery sites seem to be the most popular today, especially with small to medium-size companies. These facilities are movable trailers that are wired for telecommunications or have satellite communications for the user. The computer staff arranges to have the mobile recovery site delivered to a nearby location and computer operations are moved to this facility. Companies might use mobile recovery sites if their facility experiences water damage, sustains a loss of infrastructure in the immediate area, or needs a temporary facility during construction or renovation. Some companies are looking at mobile recovery sites as an alternative to hot and cold sites, thereby saving their employees the stress of temporary relocation during a disaster.

Protecting your data from loss is the key to your contingency plan. Continuity of operations and services is important to the survival of your organization. If you don't think about how you

will get up and running again if you can't get into your building, then you may never restore the data or the services. Most important is updating your computer disaster response plan when there are changes in operations, procedures, or programs in your computer departments at any level of the organization.

NOTE

1. Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Securities and Exchange Commission, "Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" (Washington, D.C., August 30, 2002), www.banking.state.ny.us/ce0230830.htm.