Winter 1989

Computers: Planning for Disaster

Jeanne Drewes

Computers: Planning for Disaster*

Jeanne Drewes**

Ms. Drewes recommends ways to protect computers and include them in library disaster/contingency planning. She also discusses routine backup, protection of software and hardware, insurance/ manufacturer agreements, and disaster plan updating.

> Materials other than book and paper deserve greater attention and concern as libraries and archives collect new and interesting media.
>
> —Sally Buchanan[1]

With the above statement, Sally Buchanan spotted the hole in many libraries' current disaster plans. Because library use of computer technology for cataloging, public catalogs, serials and acquisitions control, word processing, and database access is growing, it is imperative to include technology in any disaster/contingency plan.

Economics is a primary factor in a law library's decision to have a written disaster/contingency plan. While many organizations agree in theory that a written plan would be useful, it does not seem cost-effective to spend time and money planning for a catastrophe one hopes is unlikely to occur. Experience and studies have shown, however, that advance planning can improve dramatically the effectiveness of an organization's response to a disaster[2] and can help guard against the more frequent losses of information from disk crashes, accidental erasures, or the departure of knowledgeable personnel. If upper-level management supports routines that help to insure against loss, then staff will be more likely to follow these routines.

This article recommends ways to guard against loss, to provide protection, and to include computers in disaster planning. The three main

---

 This is an edited version of a paper presented at the 81st Annual Meeting of the American Association of Law Libraries, Atlanta, Georgia, June 28, 1988. It is one of the winning entries in the 1988 Call for Papers competition.

** Acquisitions/Serials Librarian, Baylor University Law Library, Waco, Texas.

1. Buchanan, *The Third Decade: Directions for Preservation Conservation*, 33 CONSERVATION ADMIN. NEWS 10 (1988).

2. Mileti & Sorensen, *Determinants of Organizational Effectiveness in Responding to Low Probability Catastrophic Events*, 22 COLUM. J. WORLD BUS. 13, 14 (1987).

systems used by libraries are discussed: mainframes and minicomputers, microcomputers (including memory typewriters), and optical disk. Because electronic technology is used in all types of law libraries, solutions ranging from the simplest and least expensive to the most complete and costly are discussed. The keys to disaster planning for computers are backup, protection, insurance, and cooperation.

Backup

Backup assures against total loss of data in the event of an electrical outage or machine failure. In order to ensure the survival of backup tapes in a disaster, all duplicate data files, software programs and documentation must be stored off-site. Too often, they are stored in the same room, right next to the hardware. When a law library uses a mainframe or minicomputer, a separate data processing department usually is responsible for running and maintaining the equipment and for making the backup tape. The library's disaster planning role is minimal. Even in this situation, however, the library should appoint a staff contact person for computer problems. The contact should confirm that, at a minimum, weekly backup, and ideally, daily backup tapes are made, and that those tapes are stored off-site along with any unique documentation.

Having the documentation in safe storage is especially important when programs have been written in-house, since replacement of such documentation is at best time-consuming. If the person who wrote the program has left the organization, it will be nearly impossible to reconstruct. Paper copy of unique data entered after a routine backup is vital to recreating work lost in a disaster, and should be retained until the next backup tape is produced. The librarian should be knowledgeable about off-site storage and help find the best environment that is financially feasible. A controlled environment for archival storage of unique data is essential for maintaining the integrity of that data.

The ideal environment for backup tapes is a stable temperature of sixty-five degrees Fahrenheit and a relative humidity of forty percent. There should be no static electricity or magnetic fields, and the air should be free of smoke or dust particulates.[3] Since it takes very little space on computer tape or disk to store information, even a speck of dust or a smoke particle can destroy data. The housing of each individual tape provides some protection against dust and smoke. These contaminants pose less of a threat in storage than do variations in temperature and humidity,

3. DeWhitt, *Long-Term Preservation of Data on Computer Magnetic Media: Part II*, 30 CONSERVATION ADMIN. NEWS 4, 4 (1987).

which can make the magnetic medium brittle and unusable.[4] The proper temperature and humidity are basically the same as those that are best for books. If there is a rare book collection housed in a controlled environment, a portion of that space might be used for archival disk storage. Bank vaults are also a good solution when the tape library is small. Bank vaults are climate controlled and secure against theft.

Security storage companies, now operating in most areas, are a possible alternative for mass tape storage, but many do not guarantee a limited range of temperature and humidity variations. This situation may be acceptable, however, if tapes are regularly rotated for reuse. If tapes are stored for longer than four months, check them for errors frequently. Tapes should be stored in their cases vertically with no weight upon them.[5] Even in less than ideal conditions, an off-site location is more likely to save information in a disaster than if the computer tapes are stored in the same building. If off-site storage is not available, then a fireproof, waterproof vault is another alternative. Such vaults are very expensive if they truly guard against heat infiltration, which is a necessary requirement to avoid tape meltdown. When buying a vault, be sure to allow enough storage space for growth.

Backup is easy in the mainframe or minicomputer environment when a data processing department is responsible. With microcomputers, however, law library personnel themselves often are responsible. A regular schedule for backup is essential to protect the information stored on hard and floppy disks. Backup magnetic disks need the same storage conditions as mainframe and minicomputer tapes. Floppy disks should be stored snugly and upright so that they do not bend.[6] Most institutions do not provide as clean an environment for microcomputers as they do for mainframe and minicomputers; in general, microcomputers do not require such rigorous environmental standards. However, physical vulnerability is greater for micros in the less controlled environment. If an institution uses both a mainframe or minicomputer and microcomputers, the same off-site storage can be used for both types of backup. On the other hand, if only microcomputers are used, then off-site backup storage may never have been considered. At the very least, backup copies should be stored elsewhere in the building or taken home by a reliable person.

---

4. *Id. See also generally* S. GELLER, CARE AND HANDLING OF COMPUTER MAGNETIC STORAGE MEDIA (1983) (National Bureau of Standards Special Publication 500-101, Washington, D.C.).

5. DeWhitt, *Long-Term Preservation of Data on Computer Magnetic Media: Part I*, 29 CONSERVATION ADMIN. NEWS 7, 19 (1987).

6. S. GELLER, *supra* note 4, at 59. *See also* Waegemann, *Disaster Prevention and Recovery*, 1 RECORDS & RETRIEVAL REP. 37, 45 (1985).

Off-site storage is not the greatest problem when addressing microcomputer backup, however; instituting backup routines that are rigorously followed is. Backup needs to be fast and easy. There are several ways to do this. If there is a limited amount of data, a backup program that uses floppy disks to back up frequently changing files can be effective.

If a large amount of data is stored on an internal hard disk, either a tape backup or a high capacity portable storage device are better choices. Either system can back up a large amount of hard disk data more quickly than a floppy disk system. While a tape backup system is less expensive, the tapes do have to be transferred back onto floppy or hard disks to be accessible. On the other hand, a high-capacity, portable, hard-disk storage device, although more expensive, can be ready to use without transferring information to a disk. A portable storage device can open up all sorts of other uses, too, such as transferring information from one branch library or office to another without telecommunication costs, or allowing employees to process information at home. If the software has been stored on a backup portable hard disk, a law library can be performing online searches after a disaster as soon as a temporary location and a computer terminal can be found. Both types of portable storage are self-contained and, thus, better protected against particulates than floppy disks, so there is less risk of data corruption.[7]

In a mainframe/minicomputer environment, safeguards and checks of data integrity are routine and written into procedures. Rotation schedules of tape backups are a part of these procedures. A set routine of backup data rotation should be part of a micro system as well. Unless the most current backup is safe in off-site storage, and unless that copy is the one used in case of primary data loss, confusion will surely result. Consequently, a regular routine of backup and rotation is essential.[8] As new software is introduced (which happens more frequently with micros than with mainframes and minicomputers), data files should continue to be kept in formats readable by that software. This allows access to information originally formatted for earlier versions if the earlier software is discarded, sold, or traded in for new. In addition, personnel turnover can make old software unusable if new personnel are unfamiliar with the programs. While paper archives can be stored for years between uses without harm, data stored in magnetic media can be corrupted without any

---

7. Bryan, *Versatile Storage: The Many Virtues of Removable Media*, 12 PERS. COMPUTING 138, 143-44 (1988). *See also* Calmes, *To Archive and Preserve: A Media Primer*, INFORM, May 1987, at 14, 16; Fruscione, *The Offline Factor: Information Storage*, INFORM, June 1987, at 20, 22; Laub, *The Evolution of Mass Storage*, BYTE, May 1986, at 161, 168.

8. Yaremko, *Make a Plan for PC Disaster Recovery*, OFF., Mar. 1988, at 54, 55.

noticeable physical damage to the media. Therefore, backup data need to be checked periodically for readability.

When floppy disks are used for backup, the quality of the disks is a paramount concern. To date, no standards have been set for archival quality magnetic disks or tapes. Vital information should be stored on high-quality magnetic material, which should be reused a limited number of times. The loss of data on old disks (on average, after three years of use) has been noted in the recent literature. While the data is still on the disk, the directory may be unreadable because of too much disk wear.[9] Even the new Teflon disks do not necessarily protect against this type of loss. While Teflon-coated disks are more durable and are made to withstand food spills,[10] to date there is no evidence that they have a longer readability life. The best advice is to use new, name brand floppy disks for archival copies until a standard has been set.

Optical disk technology can also be used for backup. With WORM ("Write Once—Read Many") technology, permanent data files can be created on an optical disk, which is much less fragile than floppy disks. The newest optical disk technology allows rewriting of information; however, the technology is expensive.[11] To date, it has not yet had the time test for archival storage durability. But, as the technology continues to improve, optical disks may become the most viable option for archival storage. Heat is a destructive force, even for optical disks. Most manufacturers, while touting the durability of optical storage, also recommend the same environmental storage conditions for optical disk as for magnetic storage media.[12]

Protection

Protection of computer information and equipment means removing hostile elements, such as water, dust, smoke, heat and humidity from the computer environment. Software is best protected by always returning the tape or disk to its storage container. For floppy disks, use the paper envelope and a closed plastic storage case;[13] for tapes, use the closed plastic casing. Storing computer disks or tapes at least a foot above the floor helps protect them against dust and static electricity from vacuum cleaners as

---

9. *The Help Screen,* PC WORLD, Mar. 1988, at 240.
10. Hawkins, *Coffee, Tea or Data?,* POPULAR SCI., Feb. 1988, at 26.
11. Savage, *Trio Vows Erasable CDs on the Way,* COMPUTERWORLD, May 16, 1988, at 4, 4.
12. Helgerson, *Optical Discs: New Storage Media for Education,* TECH. HORIZONS EDUC. J., Mar. 1987, at 50, 51; Fruscione, *supra* note 7, at 22.
13. K. LORD, JR., THE DATA CENTER DISASTER CONSULTANT 59-60 (2d ed. 1983).

well as from low flood water.[14] Using a locked case placed in an inconspicuous location will protect data from vandals and theft. Loss from fire damage can be minimized if duplicates are stored off-site; even hard disks are subject to meltdown in extreme heat. Magnetic media can be dried and cleaned,[15] but it is very expensive to do so, and there is no guarantee that the data will be saved.

Computer hardware also needs to be protected. Using a disk drive cover protects the read/write head from particulate matter contamination. Using plastic, static-free covers for the computer and keyboard when the computer is not in use not only protects the machine from particulates, but also from water damage if the water source is from above. In one instance where a roof leaked, a plastic cover saved the computer terminal from any damage, while uncovered terminals had to be replaced.

Most law libraries prohibit smoking; this certainly should be the rule wherever computers are housed. A "no food or drink" rule in the computer work area is also a protective measure against damage to the keyboard and disk drive. Such environmental protection of hardware and software will preserve the integrity of data, give longer life to equipment, and may save replacement costs in the event of a disaster.[16] Typewriters with memory chips also should be covered and turned off at the end of the day, as should terminals for laser disk access.

Printers should not be run without the cover attachment, which protects the printer from particulate matter and other foreign materials. Covers also protect equipment in time of disaster.

When there is dust and smoke, such as from construction, extra precautions should be taken when using computer equipment or memory typewriters. All equipment should be cleaned more often than is dictated by the usual routine maintenance. The most complete and expensive protection against natural disasters is to have floor water sensors[17] and smoke and heat alarms for the computer area. To be truly useful, these alarm systems must set off alarms both in the immediate area and at a twenty-four-hour security office or a local fire station. Most disasters occur when a facility is closed, so an off-site alarm is necessary.[18]

A halon extinguisher system can extinguish a fire with little damage to computer equipment, but a halon system is considerably more expensive

---

14. S. GELLER, *supra* note 4, at 9, 22.

15. Olson, *Hanging Your Software Up to Dry*, 47 C. & RES. LIBR. NEWS 634, 635-36 (1986).

16. K. LORD, JR., *supra* note 13, at 105; S. GELLER, *supra* note 4, at 19.

17. *Protecting Computers from Water*, 7 LIBR. SYS. NEWSL. 52 (1987). For a general discussion of various fire prevention systems, see J. MORRIS, MANAGING THE LIBRARY FIRE RISK (2d ed. 1979).

18. Martin, *Security in Libraries, Part III: Disaster Prevention*, LIBR. ISSUES, July 1987, at 1, 1.

than a water sprinkler system. If only a sprinkler system is available, there should be an automatic turn-off system for computers to avoid electrical shorts. A dry pipe system, which has compressed air in the pipes until an alarm releases the water valve, prevents pipe leaks. Some experts say that sprinklers are preferable to halon, and some studies have shown that halon leaves a film on magnetic tape and read heads. However, Halon 1211 is the best portable extinguisher for use around computer equipment for extinguishing small fires involving plastics.[19] The possibility that halon will not continue to be manufactured because of ozone depletion concerns, however, makes the dry pipe water system attractive.

If an automatic shutdown system is not installed, terminals should always be turned off at night. This safeguards against flood damage if a floor water sensor system is not available. A system that has been shut down can survive water contact, but a system that has been left running will be damaged by electrical shorts. A wet terminal can be dried and then cleaned with little or no damage. Even dirty water can be removed without damage to the entire machine if there was no power to the equipment at the time of initial water contact.[20]

Insurance

The degrees of protection for computer systems may influence the cost of insurance coverage.[21] A complete alarm system, for example, may allow a library to carry less than complete coverage, while minimal protection necessitates more comprehensive coverage. As a law library acquires more computer systems, it is important that insurance coverage keep pace.[22] Remember to include all peripheral equipment, such as modems and printers. An inventory of equipment and software should be stored off-site with the disaster plan to speed insurance claims and reimbursement. Be sure that you know insurance claim requirements. Some companies require pictures to assess the damage to equipment before anything is moved. Computer tapes of library holdings can be helpful in the case of a damaged collection claim, which reinforces the need for such vital information being stored in a secure off-site location. If insurance coverage is inadequate, you should secure a commitment from the parent institution to pay recovery costs.

---

19. Gast, *Protecting Computers Against the Hazard of Fire,* OFF. ADMIN. & AUTOMATION, Aug. 1985, at 50, 52.

20. Wexler, *Relectronic—Restoration Rather than Replacement,* BUS. J. N.J., Oct. 1986, at 124.

21. For a general discussion of insurance, see C. MYERS, INSURANCE MANUAL FOR LIBRARIES (1977). *See also* Fu, *Handling Water Damage in a Law Library,* 79 LAW LIBR. J. 667, 669-71 (1987).

22. Roman, *Keeping DP Risks in Hand,* COMPUTER DECISIONS, June 30, 1986, at 58, 60-61.

The other "insurance" for fast recovery after a disaster is a written agreement for replacement equipment from the manufacturer. The need for fast recovery is essential at state or firm law libraries, but even university libraries need reasonable recovery if the semester is not to be lost for the students. In a shared computer environment, it is important to establish the law library's priority for computer use. While few data processing departments will agree to put law library services at the very top of a list of essential services, it is important to be somewhere on that list, rather than on a nonessential services list, in order to have a time frame for reestablishing services. Microcomputer manufacturers and peripheral manufacturers should provide a written guarantee for replacement time.[23] If an alternative site is necessary to resume temporary operations, then replacement equipment, including modems, can mean the difference between available online, full-text database searching and no resources for research.

Cooperation

Planning takes time. A joint venture in disaster planning can save time and energy in initial planning and writing and can be of great service in time of disaster. Such mutual support groups are already in place within the data processing community in some locations.[24] Establish a cooperative agreement among law libraries for sharing computers in the event of a disaster. If you rely on mainframes or minicomputers, having a good working relationship with the data processing department will be valuable. Studies have shown that established lines of communication help in the event of a disaster.[25]

Cooperative efforts in planning and agreements to allow shared computer use in an emergency can lessen the time needed to plan and minimize the effects of disaster. Some organizations depend on "hot sites" ("backup processing facilities that are fully equipped and ready to run if an organization's primary data center is destroyed"), others on "cold" or "shell sites" ("hotsites without hardware")[26] for reestablishing computer services. Law libraries would do well to have similar plans. A cold site maintained for a number of institutions would be a cost-effective alternative. An even less expensive alternative is to agree on the exchange use of excess computer capacity as well as sharing other resources among

---

23. K. LORD, JR., *supra* note 13, at 83, 185.

24. Robbins, *No Longer the "Loneliest People in the World,"* INFOSYSTEMS, June 1987, at 38.

25. Mileti & Sorensen, *supra* note 2.

26. Roman, *supra* note 22, at 61. *See also* Kolodziej, *The Disaster Business,* COMPUTERWORLD FOCUS, June 1987, at 27, 29.

local law libraries in time of a disaster. Be sure that hardware is compatible with your system when making shared computer agreements.[27]

The Plan

The written disaster/contingency plan should have a section on computers which includes the following information: the phone numbers of responsible persons and their assigned duties and capacity in an emergency; the addresses, telephone numbers, and agreements of suppliers of computer hardware for either temporary or permanent replacement; the insurance company's representative and telephone number; a list of all software and documentation; back-up system and file-retrieval instructions; and an inventory of all computer equipment with model numbers and locations.[28] There should be a routine to update the plan periodically. The people responsible for setting the priorities in the aftermath of a disaster should be well versed in the essential recovery priorities and procedures as well as with the daily priorities essential to running the law library. A test run to evaluate procedures before a disaster will assure that the plan will work when the need arises.[29] When there is a data processing department within the organization that provides services to the library, that department should have a written disaster plan. The law library should be familiar with that plan to be sure it meshes with the law library's disaster plan.

If the organization has no disaster plan, computers may help justify the cost of writing a disaster plan.[30] People in authority often see computers as a greater investment than books, so a commitment from upper management may be more forthcoming when it is shown that computers are at risk. Be sure to work with the data processing department and any other departments that may have an impact on law library procedures in the event of an emergency.

Conclusion

The importance of computers in law libraries means that their protection in the event of a natural disaster is essential. While the best plan to cope with disaster is prevention, preparation can go a long way in

---

27. Kolodziej, *supra* note 26, at 31.

28. Mische & Hughes, *Disaster-Recovery Planning for Data Processing,* NACUBO BUS. OFFICER, Dec. 1986, at 28, 30-31.

29. Balon & Gardner, *Disaster Contingency Planning: The Basic Elements,* RECORDS MGMT Q., Jan. 1987, at 14, 15-16. *See also* K. LORD, JR., *supra* note 13, at 140; Murray, *Don't Get Caught with Your Plans Down*, RECORDS MGMT Q., Apr. 1987, at 12, 12.

30. For a workbook plan that includes an entire chapter on computers, see *Disaster Plan Workbook* (1984).

mitigating the loss to a law library when disaster strikes. A good disaster plan is coordinated with all responsible parties and divides the work load logically and efficiently. If routine backup and maintenance as well as contingency planning have been done ahead of time, greater reliance on electronic technology can actually lessen the time it takes to return to normal service after disaster strikes.

Appendix

Selected Bibliography

Association of Research Libraries, Office of Management Studies. *Preparing for Emergencies and Disasters.* SPEC Kit #69. Washington: ARL, 1980.

Balon, Brett J., and H. Wayne Gardner. "Disaster Contingency Planning: The Basic Elements." *Records Management Quarterly* 21, no. 1 (January 1987): 14-16.

Barton, John P., and Johanna G. Wellheiser, eds. *An Ounce of Prevention: A Handbook on Disaster Contingency Planning for Archives, Libraries and Record Centres.* Ontario: Toronto Area Archivists Group Education Foundation, 1985.

Batcha, Becky. "Data Center Design: Two Burning Issues: Fire Control, Air Conditioning." *Computerworld* 21, no. 28 (July 1987): 72-73.

Bautsch, Gail L. "What You Don't Know Can Hurt You." *Records Management Quarterly* 20, no. 4 (October 1986): 20-22, 24.

Berg, Kenneth E. "A Successful Equation for Protecting Computers." *Risk Management* 34, no. 9 (September 1987): 52-56.

Boockholdt, J.L. "Security and Integrity Controls for Microcomputers: A Summary Analysis." *Information and Management* 13, no. 1 (August 1987): 33-41.

Brill, Kenneth. "Catching Disasters Before They Happen." *Computerworld Focus* 22, no. 14A (April 1988): 23-24.

Bryan, Marvin. "Versatile Storage: The Many Virtues of Removable Media." *Personal Computing* 12, no. 4 (April 1988): 138-46.

Bulgawicz, Susan L., and Charles E. Nolan. "Disaster Planning and Recovery: A Regional Approach." *Records Management Quarterly* 21, no. 1 (January 1987): 18-20, 44.

Calmes, Alan. "To Archive and Preserve: A Media Primer." *Inform* 1, no. 5 (May 1987): 4-17, 33.

DeWhitt, Benjamin L. "Long-Term Preservation of Data on Computer Magnetic Media: Part I." *Conservation Administration News* 29 (1987): 7, 19, 28.

_____. "Long-Term Preservation of Data on Computer Magnetic Media: Part II." *Conservation Administration News* 30 (1987): 4, 24.

Epstein, Susan. "Implementation: Preparing the Site." *Library Journal* 108 (November 15, 1983): 2142-43.

_____. "Maintenance of Automated Library Systems." *Library Journal* 108 (December 15, 1983): 2312-13.

Fruscione, James. "The Offline Factor: Information Storage." *Inform* 1, no. 6 (June 1987): 20-23.

Gast, Bruce. "Protecting Computers Against the Hazard of Fire." *Office Administration and Automation* 46 (August 1985): 50-52, 83.

_____. "Up in Smoke." *PC* 4, no. 1 (January 1985) : 293-94.

Geller, Sidney B. *Care and Handling of Computer Magnetic Storage Media.* Washington: U.S. Department of Commerce, National Bureau of Standards, June 1983.

Gilchrist, Bruce. "Coping with Catastrophe: Implications to Information Systems Design." *Journal of the American Society for Information Science* (November 1978): 271-77.

Hawkins, William J. "Coffee, Tea, or Data?" *Popular Science* 232 (February 1988): 26.

Helgerson, Linda. "Optical Discs: New Storage Media for Education." *Technical Horizons in Education Journal* 3 (March 1987): 50-52.

"Help Screen." *PC World* 6, no. 3 (March 1988): 240-41.

Herman, L. Paul. "Fire Protection Systems Must be Properly Designed, Installed, and Maintained." *Plant Engineering* 42, no. 8 (May 1988): 99, 101.

Hoffman, Annie, and Bryan Baumann. "Disaster Recovery—A Prevention Plan for NWNL." *Records Management Quarterly* 20, no. 2 (April 1986): 40-44.

International Business Machines Corporation. *Fire Suppression in Data Processing Operations.* 1st ed. White Plains: IBM, February 1984.

Irvin, Suzanne C. "Disaster Planning and Assistance: Using Computer-Based Data." *FEMA Newsletter* (September-October 1986): 5.

Isaacson, Gerald. "Disaster Recovery Planning." *Security Industry and Product News* 9, no. 7 (July 1980): 23, 41.

Jedeed, Nidal. "Planning Ahead Can Minimize Risks of DP Disaster." *Computerworld* (November 28, 1983): 130.

Kolodziej, Stan. "The Disaster Business." *Computerworld Focus* 27 (June 1987): 27-32.

Laub, Leonard. "The Evolution of Mass Storage." *Byte* 5 (May 1986): 161-72.

Lord, Kenniston W., Jr. *The Data Center Disaster Consultant.* 2d ed. Englewood Cliffs, N.J.: Prentice-Hall, 1983.

Lowell, Howard P. "Preserving Recorded Information." *Records Management Quarterly* 16, no. 2 (April 1982): 38-40, 42.

Lundquist, Eric G. *Salvage of Water Damaged Books, Documents, Micrographic and Magnetic Media.* San Francisco: Document Reprocessors of San Francisco, 1986.

Lunin, Lois F., and Judith Paris, eds. "Perspective on Videodisc and Optical Disk: Technology, Research, and Applications." *Journal of the American Society for Information Science* 34 (1983): 406-40.

Lydon, Kerry. "Halon Adds to Fire Safety of High Value, High Risk Materials and Equipment." *Security* 25, no. 5 (May 1988): 52-56.

Marcus, Eric. "Outfitting the Computer Room." *Datamation* 32, no. 14 (July 1986): 58-62.

Martin, Susan. "Security in Libraries, Part III: Disaster Prevention." *Library Issues* 7, no. 6 (July 1987): 1-2.

McComb, Gordon. *Compact Disc Player Maintenance and Repair.* Blue Ridge Summit, Penn.: Tab Books, 1987.

Mileti, Dennis, and John Sorensen. "Determinants of Organizational Effectiveness in Responding to Low Probability Catastrophic Events." *Columbia Journal of World Business* 22, no. 1 (Spring 1987): 13-19.

Mische, Michael A., and K. Scott Hughes. "Disaster-Recovery Planning for Data Processing." *Nacubo Business Officer* (December 1986): 28-31.

Morris, John. *Library Disaster Preparedness Handbook.* Chicago: American Library Association, 1986.

_____. *Managing the Library Fire Risk.* 2d ed. Berkeley: University of California, 1979.

Murray, Toby. "Don't Get Caught with Your Plans Down." *Records Management Quarterly* 21 (April 1987): 12-41.

Myers, James N. *Insurance Manual for Libraries.* Chicago: American Library Association, 1977.

Nadler, Ellis. "Computing: Planning for Disaster." *Architect's Journal* 176, no. 43 (October 1982): 73-79.

National Fire Protection Association. *NEPA 910: Recommended Practice for the Protection of Libraries and Library Collections: 1985 edition.* Quincy: National Fire Protection Assoc., 1985.

New York University Libraries Preservation Committee. *Disaster Plan Workbook.* New York: NYU Libraries, 1984.

Northey, J. "Halon Extinguishing Agents." *Fire Prevention* 122 (December 1977): 22-24.

Olson, Nancy B. "Hanging Your Software Up to Dry." *College and Research Libraries News* 47, no. 10 (November 1986): 634-36.

Pike, Helen. "Survival Planning for Data Disaster." *Computerworld Focus* 22, no. 14A (April 1988): 27-30.

"Protecting Computers from Water." *Library Systems Newsletter* 7, no. 7 (July 1987): 52.

Robbins, Renee. "No Longer the 'Loneliest People in the World'." *Infosystems* 34, no. 6 (June 1987): 38-40.

Roman, David. "Keeping DP Risks in Hand." *Computer Decisions* 18 (June 1986): 58-61.

Savage, J. "Trio Vows Erasable CDs on the Way." *Computerworld* 22 (May 16, 1988): 4, 37.

Shapley, Bruce. "The Care and Storage of Magnetic Tape." *Data Processing Magazine* 10 (April 1968): 80-81.

Waegemann, C. Peter. "Disaster Prevention and Recovery." *Records and Retrieval Report* 1, no. 3 (March 1985): 37-48.

Wexler, Annette. "Relectronic—Restoration Rather than Replacement." *Business Journal of New Jersey* 4, no. 2 (October 1986): 124-26.

Wolff, Richard E. "Snap, Crackle and Pop." *Records Management Quarterly* 19, no. 2 (April 1985): 3-6.

Yaremko, James F. "Make a Plan for PC Disaster Recovery." 107 *Office* (March 1988): 54-55, 96.

Young, Glenn, and Andrew Clark. "Disaster Prevention and Recovery: Proposal for Control Threatens Halon Output." *Computerworld* 22, no. 28 (July 1988): PS11