7-1994

Before Disaster Strikes: 12 Steps to Minimize Computer Losses; Technology Alert, July 1994

Wayne D. Storkman

JULY 1994

BEFORE DISASTER STRIKES: 12 STEPS TO MINIMIZE COMPUTER LOSSES

by Wayne D. Storkman, CPA, MBA

Wayne Storkman provides consulting services related to computer disaster recovery audits, planning and systems documentation in San Francisco, California. He is a member of the California State Society Computer Committee and is also a member of the AICPA Information Technology Membership Section. *In this Alert, he discusses ways to reduce computer system failure or data loss. This Alert has been reprinted with the permission of the author and appeared in its entirety in the California Society of CPA's* Outlook *Magazine Supplement — 4th Annual Spring 1994 Computer Resource Review.*

The failure to have adequate disaster recovery systems can cost a company dearly. Although computer backup procedures and disaster recovery planning may seem overwhelming, they are cost-effective when the consequences are considered. The following 12 steps can help you to minimize computer system failure or data loss related to a disaster.

1. **Perform regular and complete backups.** Avoid costly downtime with regular backups of data as well as application programs, network bindery, trustee, and system files. Without complete backups, you may have to re-install, re-configure, and re-customize software. Forego incremental backups that make recovery more difficult and are dependent on multiple backups. Consider using a single tape with enough space to do nightly, automatic backups. Also, don't rely on just one backup tape or disk, which may be corrupted; institute a rotation system that generates a series of nearly redundant backups.

2. **Practice restoring from backups.** Periodically test backup procedures to ensure that your system's restore function works properly and your employees can follow through when necessary. As an added precaution, maintain a separate boot-up floppy disk and practice bringing up the system from this disk.

3. **Document backup procedures.** Make it easy for employees to perform backups and recovery with clearly documented procedures, including tape rotation schedules, periodic retensioning and introduction of new tapes. Documented procedures reduce employee training costs and provide guidelines for consistent methods that reflect management policy. Maintain a written backup log that management can review to ensure that backups are performed regularly.

4. **Store backups off-site or out of state.** While you should store daily backup tapes on-site in a fireproof safe, consider designating an employee to take home weekly or monthly backup tapes. [Editor's Note: If confidentiality of the data is a critical issue, consider password-protecting or encrypting that data before it is backed up.] Alternatively, use an outside backup storage facility with delivery services. Save quarterly or year-end backups

AICPA
American Institute of Certified Public Accountants
Information Technology Membership Section

TECHNOLOGY ALERT

in case old files are needed. At the cost of a few extra tapes or floppy disks, redundant backups stored at different locations may be a business lifesaver.

5. **Prearrange alternative computer facilities and telecommunication lines.** You can keep your business running after a disaster by establishing and pre-testing an emergency data system facility out of the area or state. With a wide-area network, you can arrange an alternative telecommunications link if existing phone lines go down. If these links are crucial, consider a satellite link as a backup, which usually does not cost until used and is less likely to be affected by natural disaster.

6. **Invest in redundant systems to store duplicate data and software.** Consider purchasing fault-tolerant systems, such as a network file server with mirroring (one controller and two disks) or duplexing (two controllers and two disks). Store critical software and data on local drives so that business functions can continue if the network drive fails. Or, consider purchasing a second identical file server and use it as a separate workstation until needed.

7. **Physically protect equipment and data.** Place valuable data equipment, such as network file servers, in a room that has adequate cooling, special fire protection and is secure against theft or vandalism. Elevate and reinforce areas around critical equipment to protect against falling objects or flooding. Use high-quality surge protectors with coils and electrolytic capacitors to prevent the destruction of hard drives and other equipment from power spikes up to 6,000 volts. In case of disaster and power outage, an uninterrupted power supply unit attached to the file server allows time for an orderly shutdown.

8. **Install and enforce network security measures.** Most network software comes with fairly sophisticated security features. Use them! Approach the security issue seriously to protect data from intruders, malicious employees or accidents. Require employees to keep passwords secret and log off computers when not using them. Carefully administer network users' access rights. The "delete," "create," "modify," and especially "supervisor" rights should be given only upon management approval. Use a callback system to verify users from remote workstations. Immediately change passwords and follow other standard procedures for terminated employees.

9. **Follow computer maintenance schedules.** Prevent potential disasters and data loss by performing routine maintenance procedures. Clean your equipment and run anti-virus programs and other diagnostic utilities to test for faulty connections and bad sectors on the hard disk.

10. **Adequately train employees.** Companies need to match their equipment and software purchases with a commitment to employee training. Properly trained employees can avert disaster and reduce the aftershocks of outside computer consultants' bills.

11. **Evaluate insurance coverage annually and maintain computer inventory lists.** When major computer system additions or changes occur, review the adequacy of your insurance coverage. At the very least, evaluate your coverage annually. Keep equipment and software inventory lists current as a basis for disaster and theft insurance recoveries.

12. **Establish a formal disaster recovery plan.** Every company and each separate department should consult with computer experts to implement and document their own disaster recovery plan. When you complete your plan, give it to your auditors. If a disaster happens, your disaster recovery plan will prove invaluable. You can keep your business up and running by restoring computer systems and data — the lifeblood of any company.

For further information, be sure to read the Information Technology Membership Section's Practice Aids *Computer Disaster Recovery Planning Guide* and *Microcomputer Security*.