NICs
Network Information Connection, a Technical e-Journal

Disaster Planning

by **Reed**Booker

All who work with computers have nightmares of disaster. That's because computers and software are among the most fragile and sensitive of articles, and often as valuable, portable and concealable as a diamond necklace. Computer disasters can come in many flavors, including fire, theft and just plain failure. *Computerworld* magazine has estimated that one in 40 computer installations will suffer a disastrous event. The most common? Water damage resulting from *someone else's* disastrous event.

Owners of consulting firms and other computer-based enterprises must put disaster planning on their lists of executive responsibilities along with getting work, performing work and collecting for work. Each of those latter three necessities depend on uninterrupted operation of facilities, equipment and manpower. Disaster planning should result in two action plans: disaster *prevention* and disaster *recovery.*

The first step to preventing a disaster is to imagine it: if something can happen, sooner or later it probably will. Steven Lewis, writing in *The John Liner Review,* a magazine about business insurance, identifies computer disasters in a typology of three: loss of data, loss of access to data, and loss of personnel.

Loss of Data

Loss of data is pretty easy to comprehend. Hardware or software failure or damage has scrambled your information or erased it. This can happen through a variety of errors: human, mechanical or electronic, or through a variety of damaging events: the roof falls in, the circuit breaker doesn't pop, water pipes break, things like that.

Loss of Access to Data

Or the information may remain intact, but you can't get to it. The computers and software may be fine, but your floor is flooded and all your power is off. A skyscraper fire in Los Angeles destroyed several floors, and months later the cleanup of smoke damaged computers and media was still going on in a professional office located *ten floors* away from the site of the fire.

Loss of Personnel

Or you lose a key employee, the one person who really knows how things work. This can be a devastating event for smaller companies where responsibilities seldom overlap. Those companies risk their success on the good health, good will and continuing employment of certain key individuals. Or companies that depend on service bureaus for billing, receivables and inventory records are at the mercy of disastrous events that may occur hundreds of miles away.

Institute for Network Professionals

Volume 5, Issue 6 • April 21, 2000

Hidden Costs of a Disaster

On the surface, disaster recovery would seem to be accomplished through a risk management program that transfers the potential risks to an insurance company. It's true that all from the smallest to the largest companies can protect themselves with programs that cover the costs of restoring property and equipment, and can even cover business overhead costs for many months.

But business owners must also prepare to recover the hidden costs of a disaster. These uninsured losses include lost market share and momentum, increased costs of a restart that will include recruiting and training, lost relationships with vendors and clients, and many specific costs arising from unique experiences.

Hidden costs and losses are the primary reason that an estimated 43 percent of all businesses struck by disaster never reopen, and why 28 percent of those that do reopen close permanently within three years, according to *Contingency Journal.*

Reducing the Costs of Disaster

Reducing the effect of those hidden costs is the responsibility of a business owner, while covering the obvious costs of a disaster is the responsibility of the owner's insurance company. The answer lies in the ability of a business to regain productivity in the shortest possible time.

Nelson Bean, whose company Evans American Corporation of Dallas specializes in disaster recovery construction for large organizations, has found that hidden losses and costs of a disastrous event are time-related. Accelerating the recovery process – even though initial costs will certainly be higher – will reduce the longer-term costs of recovery and help assure continuation of a business.

The most important element of disaster planning is to define the responsibilities of individuals in the company prior to a loss. The planning is an ongoing process with periodic updates that will involve the staff in reappraising the threats to your company, keeping the plan current and everyone reminded of their responsibilities.

Following is an example checklist for disaster planning for a small- to medium-sized computer-based enterprise:

Recovering property and equipment losses. A staff member is responsible for acquiring property and casualty insurance to protect against specific losses due to, for example, fire, theft, water damage, power surges, computer viruses, even sewer and drain backup damage. Coverage may include both repair and replacement and loss of business income.

Overhead costs during a key individual's recovery from illness or injury. A staff member, usually the owner or managing partner, is responsible for acquiring disability insurance benefiting the company.

Maintaining important data in a separate location. This can be as simple as making backup discs to take home, or putting complete backup files in a safe deposit location.

Planning a "quick exit and restart." Have an alternative location already picked out where hardware, software and specific variables can be assembled and made operational within a few hours.

Internal communications. Plan a flow of information to all members of the organization to keep them abreast of events and contingency plans. This will help maintain staff morale and motivation – the most important elements in working through trying times.

External communications. Plan which persons will immediately inform key clients, customers, suppliers and affiliates about events, recovery plans and, most importantly, possible delays. Everyone outside the company will be more understanding if they feel you have leveled with them and given them reasonable expectations of service.

The best part about a disaster plan is that the process itself helps business owners to identify potential hazards and risks, and prevent them from occurring. It's usually the nightmare that you've never dreamed could happen that does.

MIMS International, Ltd. is an insurance broker that has partnered with the Institute for Network Professionals to provide professional liability to our members. For more information call 1-800-899-1399, or e-mail your requests to mims@mimsintl.com

NICs
Network Information Connection

is published by the
Institute for Network Professionals

Prices Domestic $100/yr ($8.50 each)
Outside US $125/yr ($10.00 each)

Phone US 801 223 9444
Fax 801 223 9486

Address Please send tips, special requests, change of address, subscriptions, fullfillment questions, requests for group subscriptions and other correspondence to:

NICs
1372 South 740 East
University Office Park
Orem, UT 84097-8083

or contact us via Internet E-mail at:
info@inpnet.org

Postmaster Periodicals postage paid in Provo, UT. Send address changes to:

NICs
1372 South 740 East
University Office Park
Orem, UT 84097-8083

Staff Editor-in-Chief **Keith**Parsons
Managing Editor **Darryl**Alder
Testing Editor **Deni**Berger
Tech Support Editor **Todd**Hindmarsh
Technical Advisors **Art**Allen
SteveCrowley

Back Issues To order back issues, call Customer Relations at 801 223 9444. Back issues cost $8.50 each, $10.00 outside the US. You can pay with MasterCard, Visa, or American Express, or visit our archive at http://www.inpnet.org/nics.

The Institute for Network Professionals, in alliance with technical suppliers and organizations, makes resources accessible to network professionals worldwide by providing products, training, publications and events.