# HOW TO TAKE A COMPUTER DISASTER IN STRIDE

By Greg Hanna

When it comes to dealing with computer disasters, the ideal strategy is to continue operating right through them, even if the company's offices have been destroyed. Maintaining business continuity is critical. Companies that can't access their data for more than a few hours can suffer enormous losses and even go out of business. A study by Gartner calculated the average cost of computer-network downtime at $42,000 *an hour*—with costs running as high as $1 million or more *an hour* for companies dependent on technology, such as online brokerages. Even more pessimistic is a study by Contingency Planning & Research that found that 40% of companies that are unable to access their data within 72 hours close their doors.

Of course, the costs and risks vary enormously from company to company and industry to industry, but the key point remains the same: It's a lot smarter to try to prevent computer disasters, or at least minimize their impact, than to try to recover from them.

With that in mind, a company can judge whether it is adequately protected against disasters by answering four basic questions:

- What critical production applications do we have whose loss for an hour or more would have a significant financial impact on the company?
- Are our current systems adequately protected against power outages, employee carelessness, hackers, viruses, and natural events such as lightning and windstorms?
- How will we continue to operate if our physical offices are destroyed or rendered inaccessible?
- What is the cost of system downtime in terms of lost revenue and lost productivity?

## REVIEW IT INFRASTRUCTURE

Planning for business continuity starts with a review of IT infrastructure, including an analysis of methods used to store and retrieve information as well as a determination of how long it will take to recover data in the event of a disaster and what recovery process will be used.

This initial review should include all of the on- or off-site technologies the company depends on, including servers, Internet, wireless and wide-area network connections, applications, and other software. Basics such as up-to-date firewalls and virus protection, location and security of equipment and tape backups, password management, and related items should also be reviewed.

SURPRISINGLY, THE THREATS MOST LIKELY TO TAKE DOWN A COMPANY'S SYSTEM AREN'T VIRUSES, HACKERS, FIRES, AND HURRICANES...

When it comes to firewalls and virus protection software, the key is to ensure that updates are downloaded regularly from the Internet to individual desktop PCs, laptops, and servers. Because failure to update by just one person can jeopardize the whole operation, someone should be responsible for notifying employees about current threats and making sure the appropriate updates are actually installed.

Surprisingly, the threats most likely to take down a company's system aren't viruses, hackers, fires, and hurricanes but are such commonplace things as electrical outages and power surges, employee mistakes, accidents, hardware and software failures, improper tape handling and storage, and faulty backup. So, one of the first steps

## DON'T OVERLOOK PHONES AND FILES

Companies that do a superb job of protecting their data may still be in deep trouble if they ignore their phone system and paper files.

An approach worth considering is to have a virtual PBX (private branch exchange) service stand in if the local system is unavailable. Such a virtual PBX can instantly replicate all of the features of the company's own phone system (voice mail; call forwarding; call "follow me," which transfers calls to a predefined call list, such as cell phone, home phone, etc.) and, with VoIP (Voice over IP), can also route calls to an Internet phone or computer.

Another area of continuity planning often overlooked is the integrity of the company's paper files. Despite the talk of paperless offices, most companies are awash in paper. If the sprinklers go off, much of that paper could be turned to mush. Companies can use scanning technology to capture all of their paper documents in a digital format and then automatically index them onto online digital storage. Besides protecting the documents, such digital storage eliminates the frustration of having to search manually for lost or mislaid documents.

FOR COMPANIES THAT CAN TOLERATE NO DOWNTIME WHATSOEVER, THE ULTIMATE IN BUSINESS CONTINUITY IS A VIRTUAL OFFICE THAT REPLICATES ENTIRE IT OPERATIONS.

in business continuity planning is to address everyday, commonsense precautions:

- Check to see if surge protectors are in place,
- Make sure there is proper climate control for servers and back-office equipment,
- Install an uninterruptible power source, and
- Look for obvious dangers, such as PCs or servers located under sprinklers.

### EVALUATE COMPUTER APPLICATIONS

Once this initial review is complete, the next step is to carefully evaluate all of the company's computer applications to determine which are critical to the ongoing operation of the business. One of the greatest dangers comes from storing too much critical data on a single server. If this server goes down or is destroyed, it could take days to restore or recreate the data. Storing documents on both the hard drive and the server can help prevent this kind of disaster. Yet even this precaution may be in vain if the entire system goes down. To guard against this, it makes sense to replicate or, at a minimum, back up the company's data in a separate and secure location.

Tape backup is the most commonly used method of storing data, but there are two basic problems with relying solely on this—time to recover and ability to recover. Storing tape on-site is an invitation for disaster. A common rule of thumb is to store the tapes in a secured, climate-controlled facility at least 25 miles away from the company's offices. Even then there could be difficulty retrieving the tapes if major roads were blocked as the result of a hurricane, earthquake, or other catastrophic event.

Even if the tapes are accessible, there's still the danger that they might have been destroyed or damaged by the same disaster or that the data might not have been properly written to the tape or might have been lost or corrupted because the tapes were defective or stored improperly. Most companies reuse tapes, but they don't always reformat them cleanly.

A number of companies have gone with a far more reliable approach: online backup to a remote storage facility. In such a system, all of the company's data is transmitted periodically or continuously to the backup facility.

Some large companies have their own online backup systems with off-site storage, but for most small and mid-size companies it's more practical and cost effective to turn this responsibility over to an outside vendor. In general, such online systems cost about the same as backup tape systems, especially when you factor in time required to manage the system and train the staff, as well as the higher level of security.

Companies that require uninterrupted access to their data can look into real-time replication or high availability. This ultra-secure approach continuously monitors the company's primary servers and creates an off-site duplicate of every bit of data. If the firm's primary servers are unavailable, the off-site *secondary* servers stand in, enabling workers to access data with minimal disruption.

For companies that can tolerate no downtime whatsoever, the ultimate in business continuity is a virtual office that replicates entire IT operations and makes them available to the company at any time and from any location. If the company goes up in smoke, workers can move to other locations or to wireless computers and get right back to work. Continuity is maintained at all times.

The use of redundant data circuits, either point-to-point private lines or Internet IP, provides an additional layer of data continuity. The secondary bandwidth provider should be one whose network functions independently of the local Regional Bell Operating Company. In addition, this vendor must be able to provide redundancy for not just the "long-haul" circuit but, more importantly, for the local-loop or what is known as the "last mile," which is the distance from the bandwidth provider's point of presence to the firm's communications room.

## SELECTING AN OUTSIDE PROVIDER

Companies that opt to turn their off-site data storage over to an outside provider should make sure that the provider is fully capable of meeting their needs. Here's a checklist of questions to ask:

- ◆ How fast can the provider recover the company's data and get its operations up and running again?
- ◆ Can the provider customize the solution to the company's needs and then scale up to accommodate growth?
- ◆ Is the online backup and storage facility located at least 25 miles from the company's offices?
- ◆ Is this facility secure and state of the art (perimeter hardened)?
- ◆ Does the service provide sufficient data storage capacity?
- ◆ Does it provide redundant data storage?
- ◆ Will the sent data be protected by encryption?
- ◆ Will the data be secured so that it can't be read by the service provider?
- ◆ How good is the provider's quality control? Can they document it?
- ◆ Can they guarantee sufficient bandwidth and network reliability?
- ◆ What kind of tracking and feedback do they offer?
- ◆ Is their staff highly educated? Do they have specific expertise in business continuity?

### DETERMINE IMPACT AND COST OF DOWNTIME

The final step in the assessment is a determination of the impact and cost of downtime. This involves answering questions such as:

- ◆ In a worst-case scenario with the company's physical location destroyed or inaccessible, what is the RTO (recovery time objective)—that is, how long will it take to recover the data and get operating again? Is that quick enough?
- ◆ What is the RPO (recovery point objective)? RPO refers to the point in time where you have reasonable data. If your RPO is an hour before the disaster, then you lose an hour's worth of data. If it's a week before the disaster, you lose a week's worth of data, and so on.
- ◆ How much revenue per hour will be lost while critical applications are shut down?
- ◆ How long will it be before the company starts losing business to other companies?
- ◆ If the company's financial records are lost, how quickly can we reconstruct them?
- ◆ If data from tapes can't be recovered, what will it cost to reenter the data, assuming the company's internal policy for paper documents hasn't led to the destruction of the data?

With the assessment completed and the tolerance for downtime determined, the company is ready to create a disaster avoidance plan based on its individual needs, risk tolerance, and budget.

A complete disaster plan should include a list of local vendors that can be consulted in an emergency. Even if a hard drive is crashed, fried, drowned, or smashed, there are some vendors that can perform amazing feats of data recovery.

Finally, the plan should call for an annual evaluation from a disaster avoidance consultant. With new technology continually improving the security of data and driving down the cost, the consultant can help the company make sensible and cost-effective improvements to its systems. ■

*Gregory Hanna is president and CEO of TOSS Corporation (www.DisasterAvoidance.com), which has been providing security, network, and business continuity services since 1992. You can reach him at (888) 884-TOSS (8677) or LegalData@DisasterAvoidance.com.*