

SIEMENS

How do we turn engineers working globally
into teams delivering innovations locally?



[« Back](#) | [Print](#)

Master of disaster: Basic primer offers step-by-step recovery planning for the SMB

Mark Shurr, VP, Ada Business Technology -- Manufacturing Business Technology, 1/21/2009
11:26:00 AM



Disaster Recovery Planning may seem an abstract concept, but the need for it is critical to ensure business continuity during an interruption. An unexpected event like a flood or fire will activate an emergency plan. Presented here is a practical guide to disaster recovery, from planning through implementation.

Your first question: Why develop a plan?

Disasters come in all forms: weather storms, electrical outages, fires, and floods. Enterprises must determine the how an outage would impact the organization. It is the responsibility of senior management to determine the resources that will be invested in disaster recovery planning to ensure success.

Disasters do occur and we must be prepared to respond to them. Over the past 20, I have encountered several outages ranging from simple electrical mishaps to major disruptions spanning over a period of days. Without a plan that was thoroughly tested, there would have been severe repercussions for the business.

Help from above

A successful disaster recovery plan requires support from senior management. Without this support and cooperation of the management team, the plan will have limited effectiveness when disaster strikes.

A team needs to be established, and a manual must be developed, detailing the response to each type of event. The team should be composed of knowledgeable users and managers from all key areas, including IT. Their goal is to determine the best course of action to be taken when there is an event.

Various scenarios should be reviewed and documented. Forms should be developed that enable the business to manually record transactions for eventual update to the computer systems.

A disaster recovery manual should include these points:

- A contingency plan overview;
- Definition of short-term, mid-term, and long-term events;
- Official policy approved by senior management;
- Statement of critical resources;
- Plan to ensure critical resources;

- Well understood and accepted definition of responsibility;
- Detailed written procedures to accomplish pre- and post-disaster activities; and
- A methodology to ensure that the plan can be implemented at a moment's notice.

Short-term outages are those affecting major business components for less than a day. Mid-term scenarios typically last more than days but have a definitive end. Long-term outages are defined by the need to operate away from the primary facility.

Backup and recovery

The first step in media storage planning is to identify the information on servers and PCs and implement back-up procedures. The same back-up and recovery safeguards that apply to servers must also apply to critical PCs.

PC backup

Today there are many ways to back up PCs and servers. A few of the most economical ways of backing up PCs are USB Disk Drives and Flash Drives. These methods do an adequate job but impose security issues. A preferred approach is to use Network Drives to ensure that user data will be regularly archived.

Server backup

Traditionally, server backup was performed to tape storage devices. Over the past few years, there has been a huge increase in the amount of storage required as well as the need to provide it 24/7. Therefore, alternative approaches may need to be considered. One approach is backing up to remote back-up servers. An alternate approach is backing up data to remote data storage facilities, which was made possible by the advent of high speed encrypted internet access. Backups should be stored off site in a certified secure location.

High availability

Many organizations are not able to afford any "downtime." High Availability is now more than a buzzword: it's a requirement. HA requires virtual duplication of server, application, data, and network. Even legacy applications can be modified to support high availability solutions by journaling critical databases.

Short-term planning

Short-term disruptions to a computer center require an analysis to determine the cost benefit of implementing safeguards such as:

- Uninterruptible power supplies (UPS);
- Back-up generators;
- Alternate voice and data communication paths.

The short-term plan must include a contact list of all personnel and key vendors.

Mid-term planning

In many ways the planning and recovery process is similar to a short-term plan. Today many organizations deploy high-speed circuits for their voice and data. These lines may not be available during an outage. Enterprises should have POTS telephone lines available in case of an outage. High-speed voice and data circuits should be backed up with alternate vendors to enable rapid network migration in the event of a failure.

Consideration must be made to the availability of personnel required to respond to mid-term events.

Long-term planning

Long-Term events are the most difficult to respond to and will require temporary relocation of computer facilities and personnel. Agreements with a commercial disaster recovery firm, business partner, or remote plant must be in place and must be tested on an annual basis. Backup configurations must include comparable hardware, software, and communication network. Application keys and certificates may be required.

The business units must test their disaster recovery operational plans on an annual basis.

During a major outage, the key functional areas must be able to continue to do business.

When the site has recovered and is ready to go back online, all systems must be thoroughly tested. The data may need to be reloaded from the back-up site. There should be a predefined process to confirm that the site is ready to go live.

Conclusion

All manufacturing organizations must address the issue of disaster recovery. The best place to start is with a plan that is developed across functional areas. A committee should be established to create and maintain the plan and it must be periodically tested. Everyone involved must thoroughly understand their roles and be in a position to implement them when a disaster strikes.



[About the author:](#)

Mark Shurr, VP, Ada Business Technology, has more than 20 years experience as an IT executive, including with a Fortune 1,000 international company. He can be reached at mshurr@AdaBusTech.com

[« Back](#) | [Print](#)

© 2009, Reed Business Information, a division of Reed Elsevier Inc. All Rights Reserved.

Advertisement

Compare Prices for Business Products & Services

Find the Best Deal & Save Today!

Continue 



powered by
BuyerZone