

By Debra Littlejohn Shinder, MCSE, MVP

Business continuity is much more than just a fancy word for “backup”—although some organizations treat it that way. A comprehensive business continuity plan (BCP) requires a roadmap for continuance and/or restoration of mission-critical functions during and after a disaster, such as a fire, flood, tornado or even a disease epidemic.

Your BCP must be thought out, written down, and distributed to key personnel well ahead of any incident that could cause a disruption to your operations. Copies should be stored off-site—an obvious but often overlooked requirement. Here are 10 things a good BCP includes.

1 Analysis of potential threats

Your company’s response to a disaster will depend on both the nature and the extent of the disaster. Some threats, such as a tornado or flood, may physically destroy your IT infrastructure. Others, such as pandemic disease, affect human resources while leaving buildings and machinery intact. A cyberterrorism attack might bring down your network but not affect the functionality of the hardware or your personnel. A bombing may destroy both human life and network components. A power outage could render your equipment unusable, but do no lasting damage. Thus your plan should cover contingencies for as many threat types as possible.

2 Areas of responsibility

A key component in any crisis management situation—which is what you have during and perhaps immediately after the disaster—is assignment of areas of responsibility and establishment of a chain of command. This is no time to have department heads squabbling about who has decision-making authority. And remember that some types of disasters may result in loss of personnel (or some of your staff may be on vacation or out sick when the event occurs), so be sure to assign alternates in case some of the important players are not available.

Training of key personnel in disaster preparedness, incident management, and recovery should also be addressed.

3 Emergency contact information

Your plan should include up-to-date contact information on people and entities that may need to be contacted when a disaster occurred. This is no time to be scrambling for phone numbers. Information should be included for both internal personnel (CEO, CIO, legal advisor, etc.) and external personnel and services (police, fire, ambulance, security services, utility companies, building maintenance, etc.).

4 Recovery teams

It will take teamwork to manage the crisis itself and to put things back together once the immediate crisis is over. The BCP should appoint members of a disaster recovery team (DRT) made up of specialists with training and knowledge to handle various aspects of common disasters (safety specialist, IT specialist, communications specialist, security specialist, personnel specialist, etc.). The DRT members will work with emergency services during the disaster and should have access to equipment they’ll need during an emergency (cell phones, flash lights, hard hats, protective clothing, etc.).

A business recovery team is responsible for reestablishment of normal operations after the crisis is over.

5 Off-site backup of important data

Any good business continuity plan will address restoration of your company's important digital data if it is destroyed. Too many organizations meticulously make backups of everything and then store those backups in the server room. If a tornado, flood, or bomb destroys the building, that (often irreplaceable) data is gone, too.

You should store copies of important data on removable media that's kept at a different physical location or back it up over the Internet to a remote server, or both. Just as important, key personnel should know where it's stored and have the keys, passwords, etc., to be able to restore it to get users back to a productive state as soon as possible.

6 Backup power arrangements

Many types of physical disasters can result in a loss of electrical power, or a power outage can, itself, be the disaster. For continuity of business, your organization should plan for what to do in case of a long-term outage (more than the hour or less that your uninterruptible power supplies will keep your computers and network equipment running).

If you have backup generators in place, ensure that key personnel know how to switch to generator power and know the fuel requirements for the generators (must they be fueled or do they run off the natural gas line?), among other practical issues. Consider cost factors to determine when and for how long the generators should be run. Providing full electrical power to a building with a generator can cost much more than using the power grid, so the BCP should discuss in what situations it's better to close down operations and send everyone home rather than run on generator power, and it should define who has the authority to make that decision.

7 Alternative communications strategy

If your company's phones and/or Internet connection are down, how will you keep in touch with customers, employees who are off-site, contact emergency services, etc.? Your BCP should note which employees have cell phones and their numbers, as well as whether and where you have other methods of communicating during a widespread disaster, such as ham radios. If you run your own e-mail servers, do key employees have alternative e-mail addresses that they check regularly (home accounts or accounts with Web-based e-mail services, etc.) and are these addresses known to other key personnel in case they're needed for emergency contact?

8 Alternative site of operations

The BCP should also spell out a plan for setting up operations at an alternative location if the building is destroyed or rendered unusable by a disaster. Best practice is to have ready access to an empty facility that you can move into; a more practical (less expensive) alternative would be to move your operations to a branch office if you have more than one physical site.

The BCP should also take into consideration the estimated costs of moving, setup, and ongoing operations in the new facility.

9 Essential equipment/services backup

In some cases, you may be able to recover essential equipment and move it to a new site. In others, it may be destroyed or damaged and have to be replaced or repaired. The BCP should lay out how the equipment or its functions will be replaced (for instance, you may switch to a Web hosting or e-mail hosting service until you're able to replace your servers and get them operational again).

10 Recovery phase

The BCP should address the step-by-step process of recovering and reinstating the business operations to a pre-disaster state, including assessing the damage, estimating recovery costs, working with insurance companies, monitoring the progress of the recovery process, and transitioning the management of the business operations from the recovery team back to the regular managers.



Debra Littlejohn Shinder is a technology consultant, trainer and writer who has authored a number of books on computer operating systems, networking, and security. These include *Scene of the Cybercrime: Computer Forensics Handbook*, published by Syngress, and *Computer Networking Essentials*, published by Cisco Press. She is co-author, with her husband, Dr. Thomas Shinder, of *Troubleshooting Windows 2000 TCP/IP*, the best-selling *Configuring ISA Server 2000*, and *ISA Server and Beyond*.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) **XML**
- Sign up for TechRepublic's [Downloads Weekly Update](#) newsletter
- Sign up for our [Disaster Recovery NetNote](#)
- Check out all of TechRepublic's [free newsletters](#)
- [Disaster Recovery Plan: Manager's update checklists](#)
- [Worst practices for disaster recovery](#)
- [Focus your DR planning by using these five levels of disaster classification](#)

Version history

Version: 1.0

Published: September 17, 2007

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team