5 Essentials to Prepare for (Relatively) Easy Disaster Recovery

Many businesses are unprepared to maintain access to critical data and applications in the event of a disaster. Results from a recent Coleman Parkes Research study published by CA Technologies showed that "small companies suffer the most during periods of downtime, showing the least ability to generate revenue."[1] You can't eliminate threats to business continuity, but you can implement a Business Continuity and Disaster Recovery (BC/DR) plan that will keep your company productive. Start with these five essential best practices for BC/DR.

1. Don't prioritize "everything." Focus on mission-critical elements.

Accept it: You can't protect everything. Trying to do that will only waste time, money and resources. Identify who and what will be critical to supporting your business. Then create continuity plans for those that you cannot afford to be without. Know what you could stand to lose if your critical functions, vendors and suppliers were unavailable for a few hours, days or weeks. Also, validate that your suppliers can do what they say they can do in case of a disaster.

2. Apply the right technology to manage risk.

Look for technologies that provide cost-effective redundancies to help maintain business operations, and provide a means to maintain communications with customers and business-critical employees. Cloud-based services are well-aligned with BC/DR needs: They allow businesses to rapidly deploy technology solutions as needed and scale them down when not needed.

3. Create a communications plan.

During a disaster, it can be difficult to locate the people responsible for executing your BC or DR plans. Outline a simple, effective communication plan that will not be affected by an outage. Make sure department heads maintain up-to-date contact lists and have a centralized number that employees can call for information. Use text messaging or social media to disseminate critical information if needed.

4. Test!

The only way to validate a BC/DR plan is to test it. Otherwise, you may not discover its weaknesses until disaster strikes. Make sure the fail-over procedures are accurate and contacts up to date. Exercise your procedures every year, or more often as technologies change or new people come on board.

5. Assess risk regularly.

BC/DR is a process, not a single plan. For instance, adopting new technology may require new processes to be developed and tested. This is especially true when different platforms are required—mainframe, virtual environments and cloud computing—since different skill sets are needed to manage and recover each. Keep an eye on your changing environment and stay informed about what types of applications you need to continue planning for to maintain BC/DR.

(For more BC/DR insight and resources, visit CenturyLink's Business Continuity resource site.[2])

1 http://www.continuitycentral.com/news05513.html
2 http://www.CenturyLink.com/business/products/managed-services/business-continuation/list.html

CenturyLink™ Business