

**Free Tech Report**  
*Executive IT Info Series*

*"Virtual CTO" Tim Gillen reports on  
current business technology issues*

## **How to Create a Basic Business Technology Disaster Recovery Plan in Four Steps**

Loss of data is a common problem for businesses. Fortunately, it's a problem that can easily be avoided with the correct preparation. While devastating amounts of data can be lost during catastrophes like hurricanes, the September 11 terrorist attacks, fires and floods - it doesn't take such large events to cause a business to lose important data. It can be as simple as dropping a laptop to the floor, or a power surge that results in burning out a storage device. If you don't have your crucial data backed up, even a small situation can turn into a disaster.

If you still think natural disasters are the leading causes of data loss - and that the chances of it happening to you are pretty slim - take a look at the results from a study by Strategic Research Corporation of the leading causes of business continuity and disaster recovery incidents:

- Hardware Failures (servers, switches, disk drives, etc.) - 44%
- Human Error (mistakes in configurations, wrong commands issued, etc.) - 32%
- Software Errors (operating systems, driver incompatibility, etc.) - 14%
- Viruses and Security Breach (unprotected systems are always at risk) - 7%
- Natural Disasters - 3%

### **Establishing a disaster recovery plan can be done in the following four steps:**

1) Take a potential risk inventory. Make a list of every potential cause of data loss and the solutions to each. Your list should include losses that won't affect the business very much, and those that would shut the business down temporarily or permanently. Information Technology experts can assist you with creating the potential risk inventory - as they will have the knowledge and experience to identify possibilities that you are not likely to think of but need to plan for all the same. These IT experts will also be able discuss preventative solutions to guard against each type of potential data loss.

2) Rate each of your potential data loss situations. How likely is it for each of the items on your risk inventory to occur? Rating them in order of importance and likeliness to occur will help you determine where to focus your disaster recovery plan efforts.

3) Develop your disaster recovery plan. Go through each of your potential risks and their solutions, and determine how long it would take you to recover from the loss of data for each risk. Could your business be offline for 24 hours? A week? Depending on the nature of your business, being offline for even just 24 hours could result in your losing customers to your competition. Look at ways to reduce the length of time it would take you to recover from each type of data loss risk.

4) Put your disaster recovery plan to the test. Once you've created your plan of action for recovering lost data, you should test your solutions. A disaster recovery plan is just a plan until it can be tested and proven.

---

**Timothy Gillen** CNE | MCP  
CEO & President  
"Virtual" CTO

[AskTim@terrapiIT.com](mailto:AskTim@terrapiIT.com)