Why a Disaster Recovery Plan Is Crucial to Your Business

Oftentimes, when CEOs hear “Disaster Recovery Plan,” they are immediately overwhelmed by the perceived complexity of such an endeavor. They know they need a plan to protect their business, but don’t know where to start. Don’t be overwhelmed—a disaster recovery plan doesn’t have to be extremely complex. It simply has to include certain components, which, once established, will guarantee peace of mind with regard to the protection and continuity of your business.

Let’s start with the definition of a disaster recovery plan (DRP), sometimes call a Business Continuity Plan, with respect to IT. **The technical definition is that a disaster recovery plan is a documented set of procedures to recover and protect a business IT infrastructure in the event of a disaster, which could be a natural, environmental, or man-made disaster.** Hurricanes, tornadoes, earthquakes, severe storms, gas leaks, power failures, and even terrorist attacks are among the types of disasters that could occur.

Besides these types of major disasters, a study conducted by the Strategic Research Corporation states that these are not at the top of the list with regard to leading causes of business continuity and disaster recovery incidents. The top five are:

- 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%)

Being that modern-day business is increasingly dependent upon information technology to function, disaster recovery is associated with the recovery of information technology data, assets, and facilities in the event of one of these events.

FACT: On average, over 40% of companies without a Disaster Recovery Plan go out of business after a major data loss.

Although the losses of an IT disaster are frequently measured in monetary terms, just as important are lost time, productivity, and credibility. Your customers want your product and service, and if forced to wait may well go to your competitor.

Four Important Steps in Any Disaster Recovery Plan:

In its most simplified form, a disaster recovery plan consists of these four steps:

1) Risk Inventory—You must list each potential cause of data loss and the solutions for each. This should include small losses, as well as large losses that would close your business. You can use the disasters we've mentioned to get started.

2) Rating—Rating the likelihood and importance of the risk items will help you decide where to concentrate most when developing your plan.

3) Develop the DRP—Figure out how long it would take you to recover from the disasters on your list and try to find ways that would reduce the recovery time.

4) Test—Simulate potential disasters and implement practice procedures that have been put in place to handle them. This way you'll be sure you're prepared.

According to Michael Rickert, a Cisco Certified Network Professional (CCNP), once you have established the major goals of the DRP—minimize interruptions to normal operations, the extent of disruption/damage, and economic impact; create alternative means of operation; train staff in emergency procedures; and provide for smooth, rapid service restoration—it's time to develop implementation of the plan. **This involves discovery of the disaster, response to the disaster, and recovery from the disaster.**

During the discovery phase, Rickert lists steps such as notifying senior management and setting up the DR team; assessing the extent of the damage,

determining first steps, and estimating recovery time; updating senior management and choosing the appropriate DR procedure based on findings.

During the response phase, the DR procedure would be implemented, users would be notified, staff required for DR success would be contacted, backup site would be contacted, and vendors related to the damaged equipment would be called.

During the recovery phase, it should be determined which applications should be run and when; confirmed that all staff know their tasks; ensure that the DR team has the information they need for restoration; recover affected equipment from disk/tape/other media and verify it is functioning correctly; start normal operations and notify staff/others of recovery; review the DRP and tweak good/bad parts.

In view of all this advice, we realize that many small and midsize companies simply do not have the trained staff or a dedicated IT department to set up a viable DRP. Fortunately, outside IT management teams can be contracted to develop and set up a DRP for these companies. These professional teams are highly trained in all aspects of IT disaster and have the expertise and experience to do the job right—and protect companies from ruin should a disaster occur.

We hope this introduction to a disaster recovery plan has been helpful. Please contact Tech Solutions if you would like more information or if you would like to discuss your own DRP.

Tech Solutions can handle all your workstations, servers, network, and other devices. Our goal is to work hard to prevent problems from occurring, but when problems arise, our expert IT Support team provides a quick response.

Contact Tech Solutions at (888) 225-2672 or info@tsboston.com. Visit our website at www.tsboston.com.