

Would Your Business Survive a Disaster?

P.C. Consulting

White Paper



111 Waterloo Street, Suite 101
London, Ontario N6B 2M4

telephone: 519.439.0310
facsimile: 519.439.7198

www.pcconsulting.ca

Would Your Business Survive a Disaster?

What would you do if your offices were flooded and you found your server under three feet of water? What steps would you take if a power outage shut down your servers for more than a day? What if your premises were burned to the ground? How would you recover your data and keep your business running after an unforeseen disaster? When disasters strike unprepared companies, the consequences range from prolonged system downtime, and the resulting revenue loss, to companies going out of business completely. Of companies that experience a major loss of business data, 43% never reopen; 51% close within two years; and only 6% survive the long-term. Yet many businesses are not prepared to deal with the unexpected.

The key to surviving such an event is having a business continuity plan (BCP) in place. In plain language, a BCP is working out how to stay in business in the event of disaster.

Business continuity is sometimes confused with disaster recovery, but they are separate entities. Disaster recovery is a subset of business continuity and is defined as the process, policies and procedures related to preparing for recovery or continuation of the technology infrastructure critical to an organization after a natural or human-induced disaster.

A Disaster Recovery Plan (DRP) should include planning for the resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. So, where a BCP includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, it should reference the DRP for IT-related recovery and continuity. This article focuses on disaster recovery planning as it relates to a business' computer systems.

Disasters can be classified in two broad categories:

Natural Disasters

Preventing a natural disaster is very difficult, but it is possible to take precautions to avoid losses. Such disasters include flood, fire, earthquake, tornado, hurricane, smog, etc.

Man-made Disasters

These disasters are the most common and a major reason for systems failure. Human error and intervention may be intentional or unintentional, which can cause massive failures such as loss of communication and utility. These disasters include walkout, sabotage, burglary, virus, intrusion, etc.

The following provides a basic overview of the steps required to develop your DRP:

Step 1: Risk Analysis

The first step in drafting a disaster recovery plan is to conduct a thorough risk analysis of your computer systems. List all the possible risks that threaten system uptime and evaluate how imminent they are in your particular organization. Anything that can cause a system outage is a threat; from relatively common manmade threats like virus attacks and accidental data deletions, to more rare natural threats like floods and fires. Determine which of your threats are the most likely to occur and prioritize them using a simple system: rank each threat in two important categories, probability and impact. In each category, rate the risks as low, medium, or high.

For example, a small manufacturing company located in Woodstock, Ontario could rate a tornado threat as a medium probability and high impact, while the threat of utility failure due to a power outage could rate as a high probability and high impact. So in this company's risk analysis, a power outage would be a higher risk than a tornado and would therefore be a higher priority in the disaster recovery plan.

Step 2: Establish the Budget

Once you've figured out your risks, you have to determine what can be done to restrain them and what it would cost. Can a threat be detected before it hits? How can the potential of it occurring be reduced? How can its impact to your business be minimized? Is the cost to mitigate worth it?

For example, our small manufacturing company could employ an emergency power supply to mitigate its power outage threat and have all its data backed up daily on tapes and stored at a remote site in case of a tornado. The more preventative measures you establish upfront the better. *"Dollars spent on prevention are worth more than dollars spent on recovery."*

The results of Step 1 should be a comprehensive list of possible threats, each with its corresponding solution and cost. It is imperative that those responsible for systems management present all of these threats to upper management so they can make an informed decision regarding the potential size of the disaster recovery budget (i.e., which risks the company can afford to tolerate and which it must pay to mitigate). Unfortunately, systems management often fails to communicate the real risks for system downtime to upper management. Although it's okay for management to say no; it's not okay for the technical people not to let them know of *all* of the risks.

A good place to begin is by determining the cost of downtime to the business. How long can your business afford to be without its computer systems should one of these threats occur?

Ultimately, management has to decide which threats the business can tolerate and what kind of budget is reasonable for the business to support. However, when first developing the DRP, systems support personnel are "shooting in the dark" without knowing what kind of budget is available, so both IT and management must agree early on in the process which data and applications are most critical to the operation of the business and need to be recovered most quickly in a disaster.

The management of our small manufacturer may, for example, decide that they can only afford a budget for the emergency generators and the company will have to assume the risk of an earthquake.

Disaster recovery budgets vary from company to company but they typically run between two and eight percent of the overall IT budget. Companies for which system availability is critical are usually on the higher end of the scale, while companies that can function without it are on the lower end. However, these percentages may be too small. It's not uncommon for very large companies to spend as much as 15 percent on disaster recovery.

Step 3: Develop the Plan

Feedback from management will begin to shape the DRP procedures. If, for example, they determine that the company must be up within 48 hours of an incident to stay viable, then the amount of time it would take to execute the recovery plan and have the business back up and running can be calculated based on this time frame. It is highly recommended that the recovery systems are tested, configured and retested 24 hours prior to launching them. The recovery procedure should be written in a detailed plan or "script."

The script will also outline priorities for the recovery: What needs to be recovered first? What is the communication procedure for the initial respondents? To complement the script, a checklist or test procedure should be created to verify that everything is back to normal once repairs and data recovery have taken place.

Step 4: Test, Test, Test

Once your DRP is set, test it frequently. Eventually you'll need to perform a component-level restoration of your largest databases to get a realistic assessment of your recovery procedure, but a periodic walk-through of the procedure with the Recovery Team will assure that everyone knows their roles. Test the systems you're going to use in recovery regularly to validate that all the pieces work. Always record your test results and update the DRP to address any shortcomings.

As your business environment changes, so should your DRP. Reexamine the plan every year on a high level: Do you still need every part of the plan? Do you need to add to it? Will the budget need to be adjusted to accommodate changes to the plan? As applications, hardware, and software are added to your network, they must be brought into the plan. New employees must be trained on recovery procedures. New threats to business seem to pop up every week and a sound DRP takes all of them into account.

There is no 'one-size-fits-all' solution when it comes to creating a disaster recovery plan but I hope the information in this article has given you pause to consider steps you may want to take to ensure that your business survives in the event of disaster.

If you would like to know more about how we can help you with your disaster recovery planning, please contact us to arrange a free initial discovery meeting.