

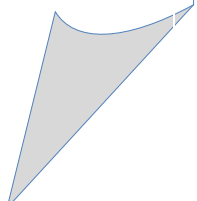


WHITE PAPER

PROTECTING YOUR BUSINESS DATA & SYSTEMS

Business Continuity & Disaster Recovery

An ISOsource Technology Brief | 2009



Executive Summary

It would be difficult to imagine a successful business organization today that is not deeply dependant on its' network infrastructure, applications, phone systems and, most importantly, data to run efficiently and effectively. There are a lot of horror stories and scary statistics that highlight the impact on companies when they lose access to their systems and data.

43% of businesses suffering a disaster never recover sufficiently to resume business. Of those that do, only 29% are still operating two years later. 93% of businesses that lost their IT functions for 9 days or more filed for bankruptcy within 1 year.¹

None of this is news to most business owners and managers. Most people are well aware of the statistics and what can happen to their business if they are not appropriately prepared. The challenge then is in how to protect yourself within the budget constraints and operating environment of your company. Disasters come not only in the form of major catastrophic events; a business disaster can be precipitated by a small local fire, major electrical issues, water flooding or damage, or other localized issues including human error. Debilitating disasters are more common than you may believe.

The purpose of this paper is to help define the objectives for most small and medium businesses with respect to business continuity and disaster recovery, discuss the alternatives available, and highlight some recommended solutions and best practices.

Summary: Companies rely on technology to conduct their business and preparing for unexpected disasters is critical to their vitality.

Disaster Recovery and Business Continuity

Let's begin with some definitions: two that get thrown around are Disaster Recovery and Business Continuity. They are related but not the same thing, the way we define these terms is as follows:

Disaster Recovery

Definition: The process that takes place during and after an organizational crisis to minimize interruption and return the establishment as quickly as possible to a pre-crisis state

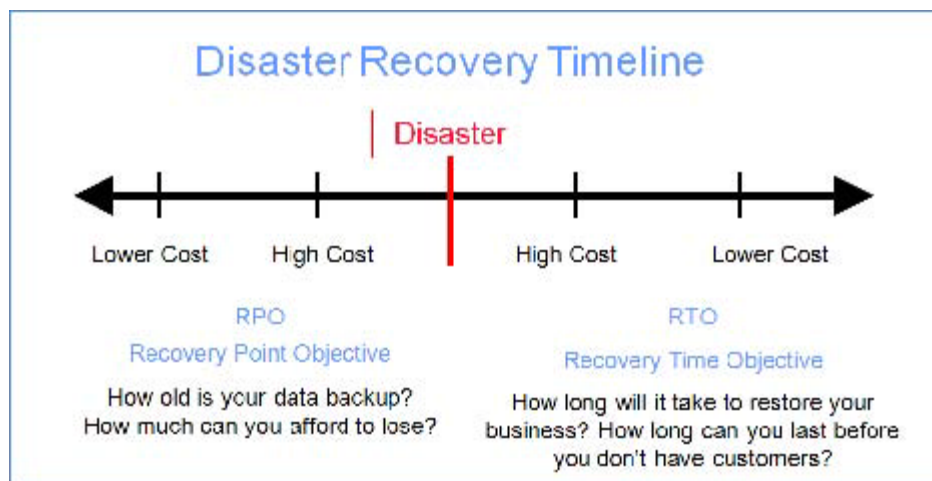
Disaster Recovery is a *reactive* process in that it is what an organization does after an incident or event occurs

Business Continuity

Definition: The process of planning to ensure that an organization can survive an event that causes interruption to normal business process

Business Continuity is *proactive* in that it consists of the processes and actions an organization engages in to keep running when an event or incident occurs

Along with Disaster Recovery and Business Continuity there are two additional terms to understand when thinking about keeping your business running after an incident occurs. These include: Recovery Point Objective (RPO) and Recovery Time Objective (RTO). These terms are best understood in the context of the timeline surrounding a disaster.



Being prepared as a business requires the right balance of proactive and reactive approaches as well as making sure your plan meets the recovery point and recovery time objectives for your organization. Let's take a brief look at the steps involved in creating a plan.

Summary: Understanding the time frame that your organization can survive without access to systems and how much data your organization can lose without severe consequences are the building blocks of a good business continuity and disaster recovery plan.

Essential Steps to Create a Plan

This document does not provide an exhaustive review of the steps and details that go into creating business continuity plans. However, there are some well understood steps that can serve as guidelines for thinking about the process and get you started in the right direction.

Step One: Initiation

The first step involves deciding to create a business continuity and/or disaster recovery plan and then kicking off the process to build it. It is important that all stakeholders in the organization support the effort, otherwise it is

likely to fail due to lack of support and funding. Conduct a kickoff meeting with senior managers and distribute a business impact analysis form (discussed in step two) to the appropriate individuals in the organization.

Step Two: Business Impact Analysis

The business impact analysis is the process that identifies the various business processes in your organization and prioritizes them for the business continuity plan. The key elements of the analysis are the amount of time that your organization can go without a specific function, for example, payroll and the cost to your organization in terms of revenue, expense, etc. of losing access to that function. People typically use higher level categories for this process versus trying to be precise as the relative impact and cost are enough for prioritization in the plan. An example of an item would be phone system. Most organizations would start to feel relatively high pain in terms of cost and impact to the organization if the phones were down for four or more hours. Upon completion of this step, your tolerance for downtime of key systems should be well understood, and the relative 'breaking points' of your business due to downtime should be identified. This data is the risk framework against which you measure costs and generate ROI analysis.

Step Three: Readiness Strategies

This is the step where you look at alternatives, determine their costs and associated requirements to implement, and select the option that best meets the needs of your organization. The recommended solution should be presented to senior management for approval and allocation of any necessary funds for implementation. It is important that you capture all the costs and ensure that the proposed solution meets the needs identified in the prior steps. Things to consider for costing:

- Data backup and all of its components
 - Data must be regularly backed-up.
 - Data should be replicated.
 - Data back-up plan should include regular testing.
- System recovery
 - Key systems identified in step two must be able to be recovered in the timeframe identified.
 - Data must be able to be restored to these systems.
- Process and workflow recovery
 - Your applications and technology are often integrated in ways that support core processes, and being able to ensure that these workflows can be restored is often overlooked.
- Facilities and telephony strategies.

Each of the above bullet points can be supported via a broad variety of methods, with differing costs. This is a lynchpin step in the planning of a business continuity plan and disaster recovery system.

Step Four: Develop and Implement the Plan

In this stage you will define the scope and priorities. This includes identifying:

People – Team members, vendors, customers, other employees, services, contacts and representatives, emergency contacts, etc.

Places – Alternate offices, processing locations, manufacturing facilities, off-site storage locations, control centers, vaults, etc.

Things – Supplies, equipment (office, computing, voice & data communications, manufacturing), vital records (business data, software, documentation, forms, references, contracts), etc.

Policy – Plan approval and execution authority, location, access, update procedure, and annual review plan, and escalation processes, etc.

The plan should clearly identify the team tasks and procedures such as emergency response, problem escalation, activation and mobilization, resumption operations, recovery operations, restoration of facilities and contents, and communications with employees and external parties (customers, vendors, partners, etc.).

Step Five: Maintenance and Testing

Once you have created a plan it is critical that you maintain it and test it. Your business needs will change over time and the plan must do so as well in order to be relevant and provide the level of security required. It is also important to test the key elements of a plan, safely and in a controlled environment, so that you know they will work when they are called upon in a real situation. It is a good idea to review the plan at least once a year.

Summary: Build your business continuity and disaster recovery plan based on an objective analysis of the value of the various processes and activities your organization performs in relation to the corresponding impact of being unable to perform those functions in the event of a disaster.

Business Continuity Solutions

The old adage that prevention is worth more than a cure holds true in business continuity. Every organization that is in business for more than a year will face incidents that they need to respond to. Most of these will be smaller in scale but they add up to lost revenue, productivity, and other damages to your business. The good news is that many of these smaller incidents can be prevented through best practices, maintenance, and putting the right products and services in place.

Securing Email

Email is one of the critical applications that businesses use to communicate. Unfortunately it is also an area where many risks exist. Many viruses are introduced into an organization through email as well as the plain annoying volume of unwanted spam. Even more potentially damaging is the use of email by organized crime and others to deliver malware and other applications that will enable them to access your systems and data.

The good news is that there are simple and effective solutions available. If you are using Microsoft Exchange for example, Microsoft has a solution that filters out spam, saving you bandwidth and also providing a layer of

business continuity in the case that your server is unavailable. Anti-virus and email archiving are two other solutions that can help secure the availability of your email. Contact your IT service provider for more information and recommended solutions.

System Security and Availability

The overall availability of your network is important and begins with putting in quality components and proper equipment. For example, ensuring the appropriate cabling is installed, electrical capacity and backup power supplies are adequate and heating and air conditioning equipment is in place to maintain appropriate operating temperatures. These are items that many people do not consider when thinking about how to make their systems more disaster resistant but can actually head off many common causes of system downtime.

The same approach applies when thinking about the firewall, routers, switches, servers and other components in your network. For example, using name brand servers (that have been fully tested with Windows Server) that have redundant systems is another cost effective way to lower the overall risk of system downtime.

A final aspect to consider regarding your system uptime is access to the Internet. Bandwidth has become incredibly inexpensive which is a great productivity enhancement, however many companies rely too heavily on only one connection, for example a DSL line. For most businesses it makes sense to have at least one backup, either a cable connection, DSL, T1, wireless or other way to access the Internet. Ask your IT consultant to conduct a network security assessment to determine if and how your infrastructure may be vulnerable to attacks and potential downtime. Your IT resource should be able to conduct a full assessment and provide recommendations based on industry best practices.

Maintenance and Optimization

Another important area to focus on that will maximize system uptime and reduce overall risk is to perform routine proactive maintenance including keeping security patches up to date. In addition, having network monitoring that is looking at the availability of systems and reporting on a real time basis is another way to head off issues before they occur. Consider regular monthly server and desktop monitoring. ISOsource offers both services at low monthly costs backed by a team of expert engineers.

Backups

This category of protection is the most critical to the overall effectiveness of your business continuity plan. At the simplest level this involves backing up the data on your servers and maybe the desktops and laptops in your organization. This is important but not sufficient for most organizations. For example, if your server were to crash and all you had was a backup of the data it would still be quite some time before you were able to be back up and running. You would need to acquire new equipment, locate the media containing all of the applications to reinstall them, make the tape equipment available for restoring the data, etc. All of this would take substantial time and in

many cases people do not have the media for all of the applications they are running which adds additional time and expense to getting back up and running.

It is also common that many companies do not regularly test their backups and often find that the files and data they thought were being backed-up are in-fact missing. When putting a backup solution together it should meet all of the following key criteria.

- Backup all systems and data, including bare metal.
- Provide quick restore of files and applications.
- Provide offsite storage for site disaster.
- Provide protection from regional disaster.
- Keep multiple copies / backups.
- Deduplication.
- Virtualization.
- Regular testing of backups.

Summary: There are many components to being prepared for a disaster, including proactive maintenance and reactive responses. Backup of data and systems is only one of the activities that should be performed for the most effective results.

Summary

If you wait for a disaster to strike before establishing a plan for recovery, you will be too late and your business will experience a loss up to and including permanent failure. Without proper plans in place, it can take weeks to recover a business, and even then, key data and systems may not be restored to their prior states: billing information and client records lost, payroll and invoicing cannot be processed, and all other business critical daily operations can be put on hold past the point that your business can sustain. A well thought out, properly implemented and annually tested and reviewed business continuity and disaster recovery plan can avoid all of this, should an unfortunate event occur.

By identifying the core requirements for bringing your business back to pre-crisis state after a disaster, and putting in place the systems and processes to execute this plan, you not only ensure the long term viability of your business, but you learn a great deal about the mission critical components of your business. Too often we take our computing systems and data for granted, not understanding the value of proper maintenance (one way to help avoid some of the more common system failures) and recovery planning.

If your business is currently without proper business continuity and disaster recovery plans and systems, we believe you are exposed to a risk that can be avoided with minimal cost and effort. Don't be caught thinking about this the day after a disaster. ISOsource has provided IT support services for over 17 years and has one of the largest local team of knowledgeable Support Engineers. Call us today and kick-start your business continuity and disaster recovery planning!

The chart below is a helpful tool to assess your readiness for a business disaster. If you answer no to one or more of the items in the chart, you likely are not prepared to recover your business from a disaster in a timely basis.

Disaster Recovery	Yes	No	?
Do you have a written business continuity plan?			
If so, have you fully tested it?			
If tested, did you pass the test?			
Have you quantified and ranked the business and financial risk of outages to all vital functions?			
Are you prepared to address liabilities and fiduciary responsibilities in case of disaster?			
Are your business continuity plans kept current and updated as business needs change?			
Do you perform regular back-ups faithfully and include every server and hard disk?			
Do you regularly send back-ups to a safe off-site archive?			
Have you standardized a proven media, drive, software, and automation back-up solution?			
Does business continuity and disaster recovery readiness have stakeholder support?			
Do you have access to the media for all business applications running?			

About ISOutsource

ISOutsource is the premier IT support services and technology consulting company for small and medium businesses in the Pacific Northwest. ISOutsource helps clients maximize business performance by delivering unparalleled experience, superior customer service, and the highest level of technical expertise all at an affordable price. Clients trust ISOutsource to provide the reliable and responsive IT support service and thoughtful consulting needed to gain the greatest business value from their technology investments. www.isoutsourcing.com - 800.240.2821.

¹ Shimberg, David. (2006) An Ounce of Prevention...Insurance Paid but the Company Failed. Retrieved December 3, 2007, from Edwards Disaster Recovery Directory Website: [http://www.edwardsinformation.com/articles/An Ounce of Prevention.asp](http://www.edwardsinformation.com/articles/An%20Ounce%20of%20Prevention.asp)