



**Business Continuity Planning:
Best Practices for Your Organization**

MCS Management Services White Paper

Changing Times, Changing Requirements

Back in the 1990s, the phrase “business continuity” wasn’t a common part of normal everyday business lexicon. What many professionals across numerous organizations spoke of was “disaster recovery.” At the time, DR as many information technology (IT) purists called it, was principally the domain of technical specialists and engineers, with limited visibility and sponsorship from corporate executives. It was something larger organizations with extensive IT infrastructures were concerned about. The focus was getting all that big hardware back up and running, in some cases within 24-48 hours, when a catastrophic event like a hurricane, flood or fire hit.

Fast forward to the current decade and what has resulted is a sea change in thinking about disaster recovery. Horrible events like Hurricane Katrina have brought heightened awareness about disaster preparedness. As a result, disaster planning in the business environment has made its way beyond the realm of IT management and onto the radar screen of more corporate executives. Along the way, information has become the lifeblood of business success. Organizations of all sizes now rely on access to mission-critical data and systems to meet business goals, service customers, and remain competitive. For many companies, being “down” for 2-3 days following a disaster is no longer acceptable when you consider the impact in areas such as lost revenue and erosion of customer confidence. As a result, the focus has shifted beyond just the recovery of IT assets (traditional DR) to one of business continuity: where people stay connected to mission-critical information and major processes keep functioning despite business disruptions.

Today, the changing regulatory landscape has also created added pressures for organizations to be prepared when the unexpected strikes. Federal regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act contain provisions that require companies to have a business continuity plan for protecting corporate records and other vital information.

When You Least Expect It....

All of these factors now make business continuity an integral issue in the success of enterprises of all shapes and sizes. It is critical to not only large multi-national companies in big industries like healthcare, financial services, and technology, but a wide range of professional services firms and small businesses as well. Many Philadelphians likely remember the infamous fire at the 38 story Meridian Bank Building, also known as One Meridian Plaza, in 1991. This horrific event impacted the operations of many service firms in the legal, banking and insurance industries, leaving them

without access to critical data and files while forcing relocation to alternate sites to continue business.

Moreover, it is not always a catastrophic event that can force a company into business continuity mode. The big disasters – hurricane, flood, fire – can wreak substantial havoc and get the most publicity, but smaller, less notable events, such as a cut power line or sewer backup can also considerably impact an organization. In today’s business environment where information is king, disaster can also come in the form of events that cut off your people from their mission-critical data and systems, like a computer network intrusion or virus.

The bottom line is disasters can happen when you least expect them to and involve almost any event that disrupts your normal business operations and threatens information access. Protecting your organization proactively through business continuity planning can be a daunting task. Business continuity is a highly specialized discipline involving a wide range of variables and complex interdependencies.

As you work toward establishing a business continuity plan, or revisiting your existing plan in the future, MCS Management Services is pleased to offer the following best practice guidelines to ease the burden on your organization:

1.) Conduct a Risk Assessment

A good starting point in the business continuity planning process is to conduct an assessment of how vulnerable your organization is to a disruption in its business operations. You should take a holistic overview of your entire infrastructure and business processes, and identify all the potential risks to your continuous operations and information access. At this stage you want to try to measure the potential impact a disruption would have on your business in key areas such as the inability to meet customer requirements and service levels; lost revenue; failure to meet regulatory requirements; and erosion in customer, investor and employee confidence.

By researching and collecting data on your resources and internal/ external requirements you will gain a better sense of any current vulnerability and how you can better plan to protect your organization more accurately and efficiently moving forward.

2.) Create a Comprehensive Plan

Building off your risk assessment, you’ll want to create a comprehensive business continuity plan that will help your organization to minimize the risk and impact a disruption can



have on your ongoing mission. The plan should address your IT assets, mission-critical software applications and systems, data protection and security, telecommunications and networking capabilities, employee requirements and processes, and supply chain relationships.

Rather than roll your own plan from scratch, it is wise to rely on readily available business continuity planning software from companies such as SunGard and Strohl Systems. These easy-to-use software tools can assist you in completing your risk assessment, and help address all aspects of business continuity planning, analysis and situation management.

3.) Back up Your Data and Files

Fundamental to every business continuity strategy is regular back-up and off-site storage of your mission critical data, documents and records. As we have noted, businesses today rely on access to mission critical information for ongoing operations and decision-making like never before. If critical data is destroyed or inaccessible as a result of a disaster, your ability to achieve continuous business operations is severely limited.

To better ensure that this does not happen to your organization, you should back-up your critical electronic data and files on a regular basis, at least a week. Data should be stored off-site through a leading information protection and storage company. You can also utilize scanning software to make an electronic copy of daily and current hard copy documents (messages, internal and external memos, client correspondence, and other) and then store these files off-site to provide your organization with added level of protection. In addition, as part of your records management program, a strategy should be put in place to store older hard copy files and documents off-site as well.

4.) Protect your Computer Networks

In today's cyber world, security threats to data and systems pop up on a seemingly daily basis. Compounding the challenge, is our reliance on e-mail as the communications method of choice in the business environment. Viruses, spam and other forms of network intrusion pose an equally compelling risk to business continuity as do physical disasters.

If this isn't enough of an incentive, regulatory requirements arising from Sarbanes-Oxley and HIPAA, legally compel many organizations to demonstrate that internal data and systems are protected against security threats. Data security can be an overwhelming task that is outside the core competency of many organizations. Fortunately,

there are readily available technologies for protecting your data and mission-critical networks from security threats. An experienced partner or consultant can help identify the right range of solutions for your organization.

5.) Facilitate Ongoing Computer Access

Backing up and protecting your mission critical data and information is only part of a comprehensive business continuity plan. In the event that a disaster denies your organization the ability to utilize your facility or office, the question arises where will you access compatible computer systems to restore the data and run required applications?

Accounting for alternate computer access is a must in your business continuity strategy. For some organizations, this may involve the use of another in-house facility or location. For others, it may require establishing a relationship with an external business continuity provider like SunGard or IBM who can provide access to one of their recovery centers (known as "hot-sites") and the computer resources you require in the event of a disaster. These companies have the experience to help you restore and run critical applications out of their facility until you are ready to re-enter your own location.

6.) Where Do Employees Go?

Historically, data and computer access have been the primary focus of disaster recovery and business continuity planning. While these areas clearly remain a critical component of today's plans, the third and equal rung in the strategy focuses on people and process. Specifically, where will your employees and staff go if disaster denies access to your primary facility or office?

To ensure that your business can resume as efficiently as possible following a disruption, alternate locations where employees can go must be identified. These locations should be equipped with the office and support resources – workspaces, desks, chairs, computers and phones – necessary to facilitate a "business as usual" environment. Again, for some organizations this may be another local office location. However, this may not be a viable solution due to office space or geographical limitations. In this case, the alternate locations can be gained through a contract with a business continuity provider. These firms have fully-equipped workgroup oriented facilities where your managers and employees can go until they are ready to return to your primary location.

7.) Account for your Supply Chain Relationships

Getting business done today often requires a wide range of third party relationships that make up an organization's supply or value chain. This includes telecommunications services, shipping and freight providers, daily mail communications, and much more. If your primary location is unavailable, where do important packages get picked up? Where does mail get delivered? These are important, but sometimes overlooked questions.

It is important that your business continuity strategy recognizes the dependencies your organization places on these supply chain relationships and how, in the event of a business disruption or disaster, service delivery can continue in the manner you require.

8.) Establish a Communications Strategy

During the time of a disaster or business disruption, communications becomes a critical component in the implementation of the business continuity plan. A strategy should be put in place for communicating with management and employees, as well as clients and outside vendors and partners, notifying them of the disaster event and what steps are being followed. A master list of all required phone numbers and e-mail addresses should be maintained off-site by a designated staff person. One designated media spokesperson should also be identified to handle any press inquiries that may result.

A well managed and consistent communications process will help to protect employee and customer confidence during a business disruption, and portray the company more favorably in the minds of the public.

9.) Test the Plan

Business continuity experts often argue that the most important element of the planning process is testing. They profess that the best-laid plans often have holes that aren't uncovered until it's too late. Testing provides the means to uncover areas of your plan that may be weak or identify aspects of your operations or infrastructure that have not been accounted for.

Regularly scheduled tests of your business continuity plan should be conducted on an annual basis, or more often if major changes (new systems, major new applications) to your infrastructure are put in place. You should test your ability to restore and operate your systems at your designated alternate location. If you establish a relationship with a business continuity provider, testing is a critical component of your contracted relationship. To test their disaster related communications strategies, some organizations even conduct "mock" disaster drills and then use the feedback to make changes and improvements.

Your Next Steps

Business continuity is a multi-faceted and complex practice. The best practice guidelines contained in this white paper are not intended to address every aspect of business continuity planning, but rather point your organization in the right direction. At MCS Management Services, we recognize the critical impact that a disaster or business disruption can have on your organization and stand ready to assist you in the business continuity planning process. **Contact us today at 1-800-473-5003.**