



Disaster Recovery and Business Resumption – Business Contingency Planning

Excerpted from Technology Best Practices
Robert H. Spencer & Randolph P. Johnston
First in a Series of Four Articles



Business Contingency planning is critical to every business and organization. The recent devastation left by Hurricane Katrina serves as another illustration of the importance of having a Business Contingency plan in place. Whether you refer to your plan as a Disaster Recovery plan or Business Resumption Contingency plan, the importance of having a plan is evident.

There is more than one approach to contingency planning. The traditional approach is to prepare a plan in case information systems fail as the result of a major storm or fire damage. These are disasters; no doubt about it, but the risk of one of these events occurring is relatively small compared to other events that happen every day. These daily events can cost a business far more than a single catastrophic failure. Contingency planning today must go further than sending backups to off-site storage, or even having a remote alternate processing site. True contingency planning is about keeping the business afloat during a number of unforeseen emergencies.

Because technology has permeated the workplace much more than a decade ago, contingency plans must focus more on the workplace and the processes performed. The plan should detail how the recovery process will take place from the human perspective. Getting the technology back online may be the least of the problems. Organizations must review their plans and update them. Organizations must go beyond their information systems and develop comprehensive contingency plans for all critical resources.

After tragic events of September 11, 2001, many organizations initiated a review of their internal contingency plans. Organizations affected by the terrorist attack that had tested contingency plans were up and running, at least at a minimal level, very quickly. Organizations must ensure they can rapidly provide a minimally acceptable level of critical services during a disaster.

As recent events have shown, organizations can experience a sudden disruption of their operations. The disruption can be minimal, with a power outage for an hour or two, or a building and its contents could be destroyed by a Hurricane (as evidenced by Katrina), a sudden explosion or fire. Threats to your business can be natural, human, or technical. To be effective, contingency plans should consider potential disasters at all levels. The plans should assume that the business could not continue operating at its physical location, due to a natural disaster or some other unforeseen event, for an extended period.

Contingency planning includes five phases:

1. Establish organizational planning guidelines.
2. Analyze business impact (the risk assessment).
3. Develop detailed contingency plans.
4. Validate.
5. Communicate the plan.

Management today must be keenly aware of how technology has caused the work environment to become very sensitive to disasters that affect that technology. Imagine, for a moment, that a business's computers, network, and servers all just go down. "What can be done next?" "What

would be the impact on the business?" The impact is different for each business, but considers the impact on a professional services firm. This could be a public accounting or law practice, or an architectural or engineering firm. These types of businesses are easy to use as an example of the cost of a failure, because they bill their clients based on hours worked. Time is the inventory, and if that inventory is not used every minute, the time can never be reclaimed for sale at a later time. It is lost!

Assume there is a staff of 100, all with an average billing rate of \$100 per hour, just to make the math easy. It is tax season, or the middle of a major case, or designing a high-rise building. How long can the business stand losing \$10,000 every hour? Perhaps this scenario is a bit over dramatic, but then again, maybe not. Most business environments today are so dependent on technology that the loss of systems for any extended period of time can be catastrophic. There have been reports of companies who never recovered from a major loss due to catastrophic failure. This failure may have been caused by simple mechanical failure, a force of nature, or a simple brownout or planned blackout.

A few years ago, one major food manufacturer and distributor was nearly shut down because of an upgrade to a new software application. The information technology department had moved forward with a significant upgrade. But, all affected departments were not aware of it. Recovery options for an upgrade failure were not properly planned. The upgrade failed. The company could continue to make its product, but trucks were waiting to deliver, and store shelves were empty. The company was so tied to its technology that it could not take orders, track shipments, or do billing.

This was by any definition a disaster – an internal disaster, caused by a failure to plan properly perhaps – but no less a disaster. Buildings did not burn, employees were ready and able to work and services were all in place. But the business could not continue in any normal capacity. Managers who think of a disaster only in terms of catastrophic failure should rethink their definition.

Watch for the NMGI October Newsletter excerpt "Managing Technology - Part One"



Contact your NMGI Sales Consultant for assistance in developing a Business Contingency plan for your organization. www.nmgi.com 620 664-6000



Additional details may also be found in [Technology Best Practices \(Wiley Best Practices\)](#)

By Robert H. Spencer & Randolph P. Johnston.

http://www.amazon.com/exec/obidos/tg/detail/-/0471203769/qid=1127161139/sr=2-1/ref=pd_bbs_b_2_1/102-9242540-7343347?v=glance&s=books
