



Disaster Recovery Planning: Top 10 Things You Need to Know

By Brett Callow and Rhonda Turner

Introduction

At best, a disaster can result in lost productivity and lost profits; at worst, it can seriously threaten the survival of a business. But by implementing a disaster recovery plan, a business can both minimize potential losses and improve its chances of survival.

This paper will provide an overview of the steps that a business need to take in order to implement an and maintain an effective disaster recovery plan.

In enterprise level businesses, disaster recovery plans (DRPs) are often inadequate or outdated and in small to mid-sized businesses (SMBs) the situation is even worse: only a relatively small percentage have any form of plan. Why do so many businesses have such a lackadaisical approach to disaster recovery planning? Probably because it's a long and complicated process that ties up key personnel, can be costly to produce, and will change over time so it has a limited shelf life. And why spend time producing a document that may well never be needed? But any businesses that ignores a DRP is gambling that disaster will not strike and gambling with the livelihood of its employees and with the investments of shareholders and stakeholders. Why take such an unnecessary gamble? Why expose your business to such an unnecessary risk?

Before we go further, it's a good idea to define what a disaster. The obvious definition would include natural disasters, such as floods, hurricanes, earthquakes and fires. In recent years, terrorist attacks have been added to the list of man-made disasters. But what about problems that only affect one company, one facility or even just one server? For the sake of this document, we will define *disaster* as any unplanned system downtime that impacts a company's productivity beyond that deemed acceptable by the IT manager. Using this definition, a disaster could include the failure of the web server for a company that sells its products online, a failure of a SQL server for a company that runs database-intensive tasks, or even a virus or malware attack on a mission-critical server or bank of servers. Of course, all other natural and man-made disasters also fall into this category.

To downplay the importance of a DRP can be costly — extremely costly. At best, a business that encounters a disaster is likely to have a sizeable hole punched in its profits; at worst, the very survival of that business can be seriously threatened. According to a report from Gartner, a leading research and advisory company, 40% of businesses that encounter a disaster close their doors within the following five years. For the 60% that do survive, the expenses that result from a loss of continuity can be significant. Systems downtime alone can put a serious dent in a business's profits. Enterprises in the U.S forfeit an enormous 3.6% of their annual revenue to system downtime. On average, SMBs incur losses of \$18,000 per hour while, in the case of enterprise level e-commerce businesses, this spirals to \$7,000,000 per hour. Add to this the losses that might be incurred as a result of damaged customer relationships and the expenses

associated with recovery, and it is easy to see why a disaster can so easily sink an unprepared business.

But not all the news is bad. Businesses can both reduce their potential financial losses and improve their chances of survival by implementing a clear and comprehensive DRP.

Developing a disaster recovery plan

A DRP is a document that outlines the actions that will be taken prior to, during and following a disaster. A DRP enables a business to minimize its losses and recover from a disaster in the shortest possible time by identifying critical systems and processes and methods by that those systems and processes could be restored and by minimizing the amount of decision making necessary following a disaster.

In many instances, it will be preferable to create a number of less complicated, business unit-specific DRPs as each business unit may have very different functions and requirements and may be impacted differently by different forms of disaster.

The following sections outline best practices for creating and maintaining a DRP and can be applied in relation to both to business-wide and business-unit-specific DRPs.

Organize the project

To kick start its DRP project, a business should:

- Clearly define the scope and objectives of the DRP project
- Determine the financial and human resources that are to be made available to the project
- Create a planning team to manage the development, implementation and maintenance of the DRP
- Set a timetable for the project

These are essential steps in the process. Clearly defining these points will help ensure that the planning team returns a DRP that fully meets with business needs, within a prescribed time and within budget.

Conduct a business impact plan and risk assessment

A business impact plan should identify a business' most critical processes and systems. In determining the criticality of processes and systems, consideration should be given to availability requirements, the cost impact of any failure to meet with those availability requirements and whether or not there are any inter-system dependencies (do other systems depend on this system or does this system depend on other systems?) Once the criticality of each process and system has been established, the planning team can then work towards creating a DRP that targets resources initially at only the most critical processes and systems.

To what risk is each process or system exposed? What is the likelihood of that risk? To plan to deal with the effects of a hurricane would be pointless unless a business is actually located in an area that is affected by hurricanes. Similarly, a business located in an area that is often affected by flooding would be foolish not to plan to deal with such as emergency.

A simple formula can be used to calculate the financial risk associated with any particular type of disaster:

$$Risk = P \times C \times T$$

Where P is the probability of that disaster affecting a business, C is the hourly cost associated with the non-availability of whatever processes and systems would be interrupted by that disaster, and T is the estimated time for those processes and systems to be restored.

Performing such a calculation for each type of disaster and each process and system and comparing the results will enable the planning team to ensure that the DRP adequately addresses the events that would expose the business to the most extreme financial risks.

Identify recovery options

What steps must be taken to get processes and systems back online? How can lost data be recovered? What operations could be relocated to a different facility or site? Which staff members can be relocated to that site? Will additional or specialist staff need to be contracted? How can computer hardware be replaced and data restored to the new hardware?

A recovery option should be identified for each critical process and system. Dependencies identified in the business impact plan should be considered too: For example, if process ABC depends on process XYZ, a recovery option must be identified for both.

Develop the DRP

The DRP is a critical document. Lack of clarity will invariably result in time being wasted and, as already mentioned in this document, time is an extremely valuable commodity. The DRP should make clear:

- **Activation** — Who is responsible for making the decision to put the DRP into action? Who is responsible for should that person be unreachable? What information will need to be provided to that person? Who will provide that information? How will teams be notified?
- **Recovery** — How will each critical process and system be recovered? Who is responsible for performing recovery operations? Do particular processes or systems need a diversity of recovery options? Who will decide that option to implement? That elements of the recovery process could or should be outsourced? What elements will need coordination and contact with other teams? To what alternative sites could operations be relocated? Who is responsible for coordinating the recovery process? Who needs to be notified when a system is recovered? Who is responsible for making that notification?
- **Rebuilding** — Once the emergency recovery process is complete, what needs to be done in order to restore completely normal operations?
- **Contacts** — What are the names and contact information for key personnel? For vendors and suppliers? For contractors to that functions have been outsourced? For offsite storage?

Communication is critical to the success of the DRP and responsibilities must be clearly defined. For example, who is responsible for providing notification to end-users of the recovery of a system? Such steps are easily overlooked, especially when recovery teams are inundated with work, but any delays resulting from a lack of communication could prove to be extremely costly.

Test the DRP

While both this section and the following sections should form part of the DRP itself (and so should be covered in the previous section), they shall be mentioned separately in this document as each is an element that often overlooked, downplayed or neglected.

Does the DRP work? How can components of the plan be tested? How often should they be tested? Who is responsible for testing? Who will examine the results? Testing is essential and the DRP should contain a schedule and details of the mechanisms to be used to test the effectiveness of recovery options.

No business should rely on a plan that is untested. While testing may be disruptive and time consuming, it's nonetheless an absolute necessity. The relatively small expense that a company incurs to test its plan should be considered an investment in business continuity. If the

company discovers that the plan doesn't work or is unreasonably complex, the cost to run the test will more than pay for itself with a plan that does work.

Train the staff

What staff will be involved in implementing the DRP? What staff will be involved in implementing recovery? What specific skills will those staff need? Who will train new hires? Who is the designated backup should that key staff trainer leave the company?

By including the answers to such questions in the DRP, a business will ensure that not only are current staff well equipped to deal with a disaster, but also that future staff are equally well equipped.

Practice recovery processes

In addition to training staff and testing the DRP, staff should also periodically practice the recovery processes and mechanisms. This will ensure that not only does the staff know what functions they are supposed to perform, but also that they can actually perform those functions. Additionally, it will help identify areas of the DRP that might be problematic or that could be improved upon.

Review and maintain the DRP

Who will ensure that the DRP is kept updated? Who will notify that person when a change occurs that might impact the DRP? Is all contact information current? Is the relocation site specified in the DRP still available? Are there now any obstacles to using that site? Could the DRP be improved?

Systems change and people change and the DRP must be updated in order to ensure the best and most speedy response to a disaster.

Prevention is better than cure

How can risks be reduced? Can security policies be improved? Can a site be relocated to put it out of the reach of the disasters that are most likely to affect it? Can the estimated recovery

times for computer systems be reduced? Can an emerging technology be leveraged to help mitigate the effects of a disaster?

Fairly minor steps can significantly reduce some risk factors. For example, establishing a maintenance schedule for equipment can reduce the P in the $Risk = P \times C \times T$ formula or providing automatic failover for a server can reduce the T.

The DRP process provides an ideal opportunity for a business to examine each of its processes and systems to look for ways in to reduce the risks that those processes and systems are exposed.

Backup your data

In addition to its people, data is a business' most valuable asset. While buildings, equipment and other assets can all be replaced, data cannot. Once it's lost, it's permanently lost, and that loss can cripple a business. According to a study called *The Cost of Lost Data: The importance of investing in that "ounce of prevention*, published by an offshoot of the Pepperdine University's Graziadio School of Business and Management in 2003, data loss cost businesses in the U.S \$18 billion per year and it can be safely assumed that that figure has increased substantially during the past four years.

The backup of data is mission critical and the DRP should carefully examine the adequacy of both current backup and backup storage procedures. But it is not just backing up the data that is important: equally important is the ease and speed with that backups can be restored back into the production environment. As already mentioned, downtime can be extraordinarily costly and so it is critical that businesses seek to ensure that both its systems and the data that those systems hold can be restored in the shortest possible time.

Creating a DRP is critical to a company's survival. Included in that plan should be the specific disaster recovery software on which the plan is based. By not specifying what software you will use to restore your system, you run the risk of creating backups that cannot be restored.

To ensure that you have a viable backup, you must use disk imaging technology rather than the legacy file-based backup approach. With a disk image, you can restore a system to a known, good working state. An image can restore not only files, but also the operating system, configuration files, network configurations, applications, data and anything else that might be stored on the physical disk drive being backed up. By creating a transportable image, you can restore your image to dissimilar hardware. In fact, with the right disaster recovery software, you don't even need to know what the replacement hardware configuration will be. This is critical

when you consider that your offsite disaster recovery servers might be located hundreds or thousands of miles from the data's original site.

Summary

While disaster recovery planning has been standard in government bodies and enterprise level businesses for some considerable time, SMBs have been slower adopters. That, however, is starting to change as legislation such as the Health Insurance Portability and Accountability Act (HIPAA) and the Expedited Funds Availability Act (EFA) requires businesses to put in place a DRP. Furthermore, to avoid disruption to their own operations, an increasing number of companies will only do business with suppliers that have a DRP. Insurers too are increasingly insisting in a DRP as a condition of coverage.

So, developing a DRP is not only advisable, it may soon be essential.

There are numerous resources available to help a business plan its DRP and a couple of relevant links are provided in the *Resources* section of this document.

About Acronis

Acronis Inc. is a technological leader in storage management software, and provides a range of server and desktop protection and recovery solutions that minimize downtime and enable businesses to get back to business as quickly as possible.

Acronis True Image enables backups to be created and restored in a matter of minutes (reducing the T in $Risk = P \times C \times T$). Backups can be restored to bare metal or to dissimilar hardware and can be easily migrated between physical and virtual environments (physical-to-virtual (P2V), virtual-to-virtual (V2V), virtual-to-physical (V2P) and physical-to-physical (P2P) migrations are all supported) providing IT professionals with a wide range of backup and recovery options.

To find out more about how Acronis products can help enhance your business's DRP and provide rock solid protection for critical corporate data, visit the website at www.acronis.com or by e-mail at info@acronis.com.

Resources

Disaster preparedness strategies for small businesses (from Office Depot):

<http://www.officedepot.com/promo.do?file=/promo/disaster/main.jsp>

Contingency Planning Guide for Information Technology Systems (from National Institute for Standards and Technology):

<http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>

To find out more about Acronis True Image products:

Call +1 877 669-9749
E-mail sales@acronis.com

For OEM inquiries:
Call +1 650 875-7593
E-mail oem@acronis.com

About the authors

Brett Callow and Rhonda Turner are technical consultants providing services to a number of leading international technology companies and have been extensively involved in the planning of various industry standard IT certification examinations. Brett has been awarded Microsoft's Most Valuable Professionals (MVP) designation for the last 3 years. MVPs are exceptional technical community leaders from around the world who are awarded for voluntarily sharing their high quality, real world expertise in offline and online technical communities by Microsoft.

CA-05