BUSINESS RESILIENCY

Four Pragmatic Approaches Towards Becoming More Resilient To Business Disruptions

Written by J.R. Arredondo and Duan van der Westhuizen
Product Marketing, Rackspace®

RACKSPACE® HOSTING | 1 FANATICAL PLACE | SAN ANTONIO, TX 78218 U.S.A

rackspace®
the open cloud company

Table of Contents

rackspace®
the open cloud company

1. Introduction

An important responsibility of managers and leaders of organizations that depend on IT for their operation is to manage the risks of failure or disruption of the IT infrastructure. Disruptions are costly and can threaten the reputation of an organization and in many cases its very survival. In 2010, Forrester's Disaster Recovery Journal found that the average time to recover IT operations after a disaster or major disruption was 18.5 hours, with an average amount of data loss equivalent to 4.8 hours. Unless specifically contracted, this unplanned downtime is typically not the responsibility of the hosting provider.

Disaster Recovery (DR) is an established discipline that seeks to promote processes and policies to enable an organization to continue to operate its IT infrastructure in the face of disruption. These policies and procedures are based on strategic determinations of recovery time and recovery point objectives, and vary in the degree of protection, automation and investment required. They range from simple data backups to sophisticated integrated solutions that automate the process of restoring systems and applications in order to achieve zero or near-zero data loss.

Given the history of the discipline of DR (and overall Business Continuity), it is sobering to learn that only about a third of all organizations has an integrated business resiliency plan. It is even more surprising to learn that there are gaps between what organizations believe they are ready for and the reality of what they are prepared to face. For example, a high proportion of organizations believe they are ready to manage the IT risks related to data loss, but only a small proportion of these organizations have actually performed tests that include business users.

WHY ARE ORGANIZATIONS NOT PREPARED FOR BUSINESS DISRUPTIONS?

There are many reasons why these approaches and disciplines have not achieved broader adoption, but cost and complexity are two common ones. Many organizations, particularly those of small and medium size, simply cannot afford the time and consulting costs associated with these initiatives. In addition, the skills required to formulate and implement an effective plan against disruptions may go beyond the capabilities available to those organizations. Informally, we have heard of customers who complain that they cannot afford to invest 20 to 40% in additional costs on top of the cost of procuring and deploying a new application.

Disaster Recovery measures appear impractical because they are seen as a top-down initiative. They fail to become part of the work that people across the organization already do. This is telling because while most people believe that disasters happen as a result of earthquakes or tornados, the reality is that the most common source of disruptions are human errors or system patches.

2. Becoming More Resilient to Business Disruptions

While there are instances where natural disasters happen and do create organization-wide disruptions, it is more common that disruptions are local to a specific part of an organization. Typically, these disruptions are due to incidents that impact a specific application or workload, or a specific class of applications such as those that depend on a particular piece of infrastructure.

At Rackspace, we believe that organizations can and should take steps towards business resiliency with a pragmatic and cost-effective approach rather than avoid the issue altogether. We propose the following four ways for an organization to make progress towards becoming more resilient to disruptions.

FOUR PRACTICAL APPROACHES TO BUSINESS RESILIENCY			
Focus on the workoad	Focus on the application architecture	Focus on the application	Focus on the scope

Focus On The Workload

One of the most effective ways to provide clarity about the potential risks and their effects on the organization is to identify the workload that is being protected. By focusing on a specific workload, one is in better position to understand the scope and therefore the complexity of any potential resiliency plan. In addition, because workloads tend to have specific groups of people or teams tasked with their management, it is possible to decentralize the plan and assign its responsibility to those teams.

One example of a workload may be e-commerce infrastructure. Typically, such infrastructure includes hardware, cloud providers, applications, and teams that serve different aspects of the e-commerce function, from catalog management, to campaigns, to inventory management, to product delivery and payment processing.

All of these parts of the e-commerce function are tied together by the business process itself. This business process encompasses the catalog on the website and the order capturing system, as well as post-order processes such as payment collection, order fulfillment and product servicing. Using the business process of the workload as the blueprint, one can more easily identify those areas of risk and how those can be mitigated.

At Rackspace, we take pride in the close relationship between our Technical Support representatives and our customers. This tight relationship enables Rackspace to learn about our customers' business operations and their infrastructure, and as a result helps us provide expert advice and best practices on how to minimize disruptions.

Focus On The Application Architecture

Another effective way to provide business continuity in a practical way is to focus on applications that share the same technical architecture. It is possible for different people across the IT operations organization to come together and identify the areas of opportunity within a given stack because each brings different skills and expertise.

As an example, think of the traditional 3-tier web application. This framework is very common: in a highly simplified picture, a typical application consists of a firewall, a load balancer, a set of application servers and web servers, databases and the set of networks that connect them together. 3-tier applications that fit this model face common challenges. For example, databases may need to be replicated, or the configuration of the web server must be known and "stamped" on new servers when a server fails, just to name a couple of considerations.

Another example is those applications that run on virtualized environments powered by VMware®. Rackspace **VM Replication** enables administrators to replicate selected VMs (virtual machines) across Rackspace data centers. It's a cost-effective business continuity tool that provides geographical redundancy and helps protect and recover VMs. The VM Replication solution is available to all **Managed Virtualization** customers who are running servers that are virtualized by VMware and managed by Rackspace.

Again, because these applications share common technical and architectural patterns, it is then possible to leverage expertise and plans to ensure protection against disruption across all of them, minimizing the incremental cost and burden on the organization. We see many of our customers implement these architectures using Rackspace services, both on dedicated hardware and in the cloud. This has allowed us to create a wealth of knowledge regarding how these applications operate, and optimize our infrastructure and design our services in order to reduce the possibility of failure of the components and the networks that connect them.

Focus On The Application

Many applications that organizations depend on are not custom developed, they are packaged applications procured from third-party vendors. Each one of these applications has its own business scope, level of adoption across the company, relative importance, risk profile and technical architecture. Application vendors and cloud infrastructure providers have broader experience across many customers, and this knowledge can be easily captured to inform the specific business resiliency plans.

Take the case of Microsoft® SharePoint®. SharePoint encompasses many different areas of functionality for information workers' productivity, including collaboration, internal and public sites, content management, search, and business intelligence. Because of this breadth of functionality and its integration with Microsoft Office, SharePoint has become very popular in organizations of all sizes. Additionally, starting with SharePoint 2007 but increasingly more with SharePoint 2010, professional developers have started to see SharePoint not just as a productivity platform, but also as an application platform on which to create custom solutions.

SharePoint has its own very unique characteristics. The information architecture is based on site collections, under which there may be many different sites. These sites may have different business needs, risks and therefore many different levels of protection needs. Documents and lists data are stored in a SQL Server database that can be used to restore the content into another site if necessary. In addition, new custom-built applications can be installed to customize SharePoint for specific business needs.

Rackspace SharePoint administrators know their users' information design and priorities very well, but also have experience with the underlying technical architecture of SharePoint itself and all of the different models in which resiliency can be achieved, from data backups, data replication across farms, replication of different types of content (lists, workflows, site collections, content libraries, etc.).

By leveraging this expertise, we take steps to reduce the possibility that operations that depend on SharePoint could be affected by a disruption. We use the same approach for other third-party applications such as Microsoft Exchange and SQL Server databases.

Focus On The Scope

Finally, the most basic way to think about avoiding a business disruption is to think about the scope of what is being protected. Many problems can be avoided by the simple act of backing up an important file or creating a snapshot of a server. On the other extreme, more complex solutions are required for larger scopes.

By thinking about the scope of protection, one can identify the person or team that can most effectively implement the required protection plans, while also implementing a cost-effective plan for that given scope. From protecting important files, to protecting all servers, or the databases, or whole applications, to business services, to data centers, to cloud information, each scope helps you highlight what is protected as well as what is not.

Clearly, the maturity level of the organization in terms of its approach to business resiliency is correlated with broader scopes and more sophisticated business continuity approaches.

3. Conclusion

Disaster Recovery is an important discipline for all organizations that rely on information technology. While mature, DR has not reached broad adoption due to its cost and complexity. Instead of ignoring the problem, we propose that organizations take a practical approach to business resiliency. We recommend that organizations that currently ignore these risks should instead focus on workloads, application architectures, specific applications and simple scope-based measures to make progress towards minimizing business disruptions.

At Rackspace, we provide multiple levels of service management, from do-it-yourself on the cloud, Managed Cloud, to dedicated and fully managed infrastructure. Your organization may not have the resources or the breadth of expertise that Rackspace has accumulated over the years by servicing thousands of customers. But that does not mean that you should neglect the risks that your applications face. Practical approaches can go a long way towards ensuring an appropriate level of resiliency.

Finally, if the time has come for you to seek a cloud partner, Rackspace can help you make the transition towards a business-resilient service. From simple but effective solutions such as server snapshots, managed backups and storage services such as **Cloud Files**, **Cloud Backup** and **Cloud Block Storage**, to complex geographical redundancy using **VM Replication** for fully managed servers that are virtualized by VMware, Rackspace has a rich variety of solutions for your business resiliency needs.

DISCLAIMER

This Whitepaper is for informational purposes only and is provided "AS IS." The information set forth in this document is intended as a guide and not as a step-by-step process, and does not represent an assessment of any specific compliance with laws or regulations or constitute advice. We strongly recommend that you engage additional expertise in order to further evaluate applicable requirements for your specific environment.

RACKSPACE MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS DOCUMENT AND RESERVES THE RIGHT TO MAKE CHANGES TO SPECIFICATIONS AND PRODUCT/SERVICES DESCRIPTION AT ANY TIME WITHOUT NOTICE. RACKSPACE RESERVES THE RIGHT TO DISCONTINUE OR MAKE CHANGES TO ITS SERVICES

OFFERINGS AT ANY TIME WITHOUT NOTICE. USERS MUST TAKE FULL RESPONSIBILITY FOR APPLICATION OF ANY SERVICES AND/OR PROCESSES MENTIONED HEREIN. EXCEPT AS SET FORTH IN RACKSPACE GENERAL TERMS AND CONDITIONS, CLOUD TERMS OF SERVICE AND/OR OTHER AGREEMENT YOU SIGN WITH RACKSPACE, RACKSPACE ASSUMES NO LIABILITY WHATSOEVER, AND DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO ITS SERVICES INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.

Except as expressly provided in any written license agreement from Rackspace, the furnishing of this document does not give you any license to patents, trademarks, copyrights, or other intellectual property. Rackspace, Rackspace logo, Fanatical Support, RackConnect, and/or other Rackspace marks mentioned in this document are either registered service marks or service marks of Rackspace US, Inc. in the United States and/or other countries. OpenStack® and OpenStack logo are either registered trademarks or trademarks of OpenStack™, LLC in the United States and/or other countries.

All other product names and trademarks used in this document are for identification purposes only to refer to either the entities claiming the marks and names or their products, and are property of their respective owners. We do not intend our use or display of other companies' tradenames, trademarks, or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.