HOUTKIN
CONSULTING, INC
TECHNICAL PROJECT MANAGEMENT
PROCESS ENGINEERING

WHITE PAPER

Disaster Recovery Best Practices

Disaster Recovery Best Practices

Introduction.

Are there really best (technical) practices for Disaster Recovery? I believe there are technical and operational processes that we can look at and possibly integrate into existing production-related processes that can support the fail-over process from the production to the disaster recovery environment. I believe, as well, that a second look at aspects of the production technical environment may help to support the fail-over from production to disaster recovery. A few tweaks may be all it takes for your environment to better support the fail-over of your environment.

So, we shall embark on a journey of technical and operational process in this article, looking briefly at all aspects of the environment and process that maintains it. Perhaps you may find something that you can take back to your environment to better support your fail-over process, the readiness of your disaster recovery environment.

We must remember that there is no automatic solution for fail-over from one environment to another-even if your architecture is primarily load balanced. Failover occurs on many levels of the OSI Model. Although there could be failover built into your system using DNS you still need to understand how your application works and if can truly support a load balanced architecture. Sometimes processes can only run on one environment at a time. The same with synchronous or asynchronous replication. At some point, you need to promote or change the identify of the alternate repository to that of primary. If you look closely, you'll see that there are a myriad of mixed manual and automatic technical and operational processes that support fail-over, but it is still the human element that makes the business decisions, performs and controls the technical process. We can no longer assume that certain staff or skill-sets will be available to perform the sub-processes that support failover. The more catastrophic the event, the greater the chance that staff will not be available to count on. In fact, we cannot keep staff from responding to the event as they need to and we cannot keep staff from their family - in most cases, the balm that soothes the soul and helps the Corporation to maintain resilience without worries about retention.

How the Disaster Recovery Best Practices Series of Articles is Organized.

This article will attempt to look at six areas where best practice may be gleaned, created or integrated into existing process:

The Enterprise.

Part 1: Preliminaries

1. Best Practice No. 1: Maintain Management Support for the Business Continuity and Disaster Recovery programs
2. Best Practice No. 2: Maintain Your CIO's Vision in Your Technical Solutions
3. Best Practice No. 3: Foster a Technical Organization that Supports Disaster Recovery
4. Best Practice No. 4: Liaise with the Business Continuity Team in Support of the Business
5. Best Practice No. 5: Maintain Good Relations with the Business
6. Best Practice No. 6: Create a Incident Management Team if None Exists
7. Best Practice No. 7: Ensure Disaster Recovery Participation in the Incident Management Team

Part 2: Safety First

8. Best Practice No. 8: Create a Staff Accountability Methodology and Process
9. Best Practice No. 9: Engage an Emergency Notification System
10. Best Practice No. 10: Work with Your Building Management
11. Best Practice No. 11: The Human Resources Factor
12. Best Practice No. 12: Educate Your Community - Regularly

Part 3: Business Continuity Planning and Risk Assessment

13. Best Practice No. 13: The Disaster Recovery Process

14. Best Practice No. 14: The Risk Assessment and the Disaster Recovery Process
15. Best Practice No. 15: The Business Continuity Plan and the Disaster Recovery Process
16. Best Practice No. 16: Identify Your Worst Case Scenario and Understand the Implications
17. Best Practice No. 17: The Data Backup/Retrieval Process and Replication Methodology
18. Best Practice No. 18: Identify The Fail-over Process
19. Best Practice No. 19: Split Staffing

Part 4: Disaster Recovery

20. Best Practice No. 20: The Disaster Recovery Process
21. Best Practice No. 21: Best Practices for the Infrastructure Teams
22. Best Practice No. 22: Best Practices for the Development Teams
23. Best Practice No. 23: Best Practices for Desktop Engineering
24. Best Practice No. 24: Best Practices for the Alternate Seating Site
25. Best Practice No. 25: Best Practices for the Alternate Data Center
26. Best Practice No. 26: Create the Disaster Recovery Plan
27. Best Practice No. 27: Operational Processes and procedures supporting fail-over
28. Best Practice No. 28: Create and and Commit to the Disaster Recovery Testing Program
29. Best Practice No. 29: Commit to Quality Documentation
30. Best Practice No. 30: Practice, Practice, Practice

The Small Business.

Part 1: Preliminaries

1. Best Practice No. 1: Look at Your Business: How do you generate revenue?
2. Best Practice No. 2: Perform a Risk Assessment: What Situations Could Potentially Result in Lost Revenue
3. Best Practice No. 3: Create the Plan Mitigating Risk for Each Situations
4. Best Practice No. 4: Create a Incident Management Team if None Exists
5. Best Practice No. 5: Ensure Disaster Recovery Participation in the Incident Management Team

Part 2: Safety First

6. Best Practice No. 6: Foster a Secure Environment at Work
7. Best Practice No. 7: Create a Staff Accountability Methodology and Process
8. Best Practice No. 8: Engage an Emergency Notification System
9. Best Practice No. 9: Work with Your Building Management
10. Best Practice No. 10: The Human Resources Factor
11. Best Practice No. 11: Educate Your Community - Regularly

Part 3: Business Continuity Planning and Risk Assessment

12. Best Practice No. 12: The Risk Assessment and the Disaster Recovery Process
13. Best Practice No. 13: The Business Continuity Plan and the Disaster Recovery Process

Part 4: Disaster Recovery

14. Best Practice No. 14: Identifying tools that support your ability to Generate Revenue
15. Best Practice No. 15: The Data Backup/Retrieval Process and Replication Methodology
16. Best Practice No. 16: Identify The Fail-over Process
17. Best Practice No. 17: Putting It All Together
18. Best Practice No. 18: Practice, Practice, Practice

The Magic Bullet.

. . . . . does not exist. I am sorry to tell you that there is no device, no software out there that will respond to Disaster Recovery planning, deployment and testing. You have to simply do the work. However, your understanding of your technical environment will be vastly improved - as well as your ability to sleep at night, along with the CTO and CIO.

Business Continuity/Disaster Recovery: What is the Difference.

I am not a Business Continuity specialist. I am a Disaster Recovery specialist. However, I see both Business Continuity and Disaster as a single process. In the Business Continuity process, the Business Continuity Analyst works with the Business to gather their requirements, to document their process, to analyze the process for risks and to delineate a plan for the business based on the Scenarios that impact their mission critical business process. The Disaster Recovery specialist reviews the requirements via the Plan and is tasked with turning the Business requirements into logistical and technical solutions. The bridge between the Business Continuity and Disaster Recovery is the set of requirements, the risks, the analysis from the Business Continuity side and then the presentation back to the Business of the solutions that undergo a regular testing program.

This article refers to Disaster Recovery processes and procedures. It will mention some of the information that is gathered by the Business and the manner by which it is distributed as well as the relationships between the Business Continuity and Disaster Recovery teams. I believe that we are one large team - perhaps separated by two distinct disciplines and production technical process - but it is imperative that the Business Continuity and Disaster Recovery teams complete this single process and help each other towards a viable set of solutions and processes that support the business and keep it resilient.

Nomenclature: “Disaster Recovery” or “Alternate”.

The term, Disaster Recovery, suggests a point-in-time. The time and resource requirements cannot be mustered in time to meet those Business recovery time objectives of 0 hours or 0-4 hours - especially in a catastrophic event. With that in mind, we are looking at ways to technically keep both production and disaster recovery environments hot but hot in degrees -- to keep within a the realm of cost efficiencies. With that in mind, we are now hearing the disaster recovery seating and data center sites referred to as “Alternate” sites and will use this term to make our point. To elevate a site to “alternate” has direct technical implications and is so defined by certain technical solutions in place to make it alternate - as site that can be utilized as part of the production business process - as opposed to disaster recovery which implies use during one point in time.

The Difference Between The Enterprise and Small Business.

With regards to Business Continuity and Disaster Recovery, the primary difference is the layers of Management and the number of people supporting the business. In a Small Business, it can be one person, not a Board or 5 layers of Management that makes the decision to deploy a Safety, Business Continuity plan and related disaster recovery solutions to turn the plan into reality. There is a also a consideration of money that needs to be defined. The Small Business must be efficient in its use of funds and find the best processes and tools that support the plan.

A Note About Notification Systems.

I do not make recommendations for any systems or solutions in the marketplace. But I do recommend that every company have an emergency notification system. This system should be able to reach everyone - based on the viability of the wireless network that is engaged.

With these things in mind, I shall present each of the Best Practices on a weekly basis. On the whole, if they get you to stop and think for a moment - about your business, the people who work for you and how both could work resiliently or at least recovery from a disaster, then I have done what I have set out to do.

A Note About Documentation Systems.

I do not make recommendations for any systems or solutions in the marketplace. When I come into a new environment, there is usually so much work to do that when we come to documentation templates that we are happy with, I usually leave that to the client to determine. However, I will note that there is certain information that you absolutely, positively need to have documented. If you find a solution in the market-place that suites your needs, fine. But make sure that it provides value to you, your team and Management. As well, remember that the system will not automatically maintain the technical documentation. You will still need to ensure that maintenance of your technical documentation is responded to by adding technical Documentation Specialists to your organization or working through this requirement with your existing technical staff.

Awareness: Create a plan that works.

Whether you are a large corporate or small business, as CEO, you must be aware of the toll that stress can take on your staff and hinder your best laid plans to continue to generate revenue. Take the time to know who can handle a disaster event and who cannot. And most importantly, to not apply a stigma to those who would prefer to stay out of the event and focus on their family. You may have this need as well. This is the most difficult part of creating a plan. There are great plans out there but when it comes to an event, they fall apart because Management and Staff would prefer to be elsewhere. Be honest with yourself and your Staff. Create a plan that works and can be followed.