



Hot and Cold Site for High Availability



Common Types of Disaster

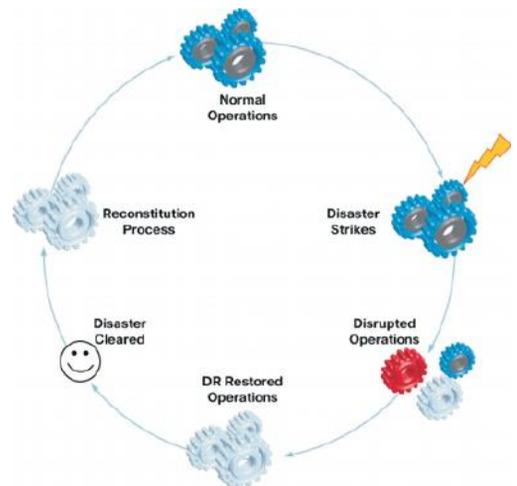
- ☞ Power outages 28%
- ☞ Hurricanes 6%
- ☞ Storm Damage 12%
- ☞ Fires 6%, Floods 10%
- ☞ Software Error 5%
- ☞ Hardware Error 8%
- ☞ Power surge/spike 5%
- ☞ Physical Attack 7%
- ☞ Earthquake 5%

Disaster Recovery

Disaster recovery is the area of security planning that deals with protecting an organization from the effects of significant negative events.

Significant negative events, in this context, can include anything that puts an organization's operations at risk: crippling cyber-attacks and equipment failures, for example, as well as hurricanes, earthquakes and other natural disasters.

Recovery Planning



Introduction

A disaster recovery plan covers both the hardware and software required to run critical business applications and the associated processes to transition smoothly in the event of a natural or human- caused disaster. To plan effectively, you need to first assess your mission- critical business processes and associated applications before creating the full disaster recovery plan. .

What is a Disaster Recovery Plan?

Disaster Recovery plan usually contains the procedures, steps, people roles, responsibilities, escalation procedures, automation processes, applications, data, IT devices and recovery priorities that are necessary to restore the damaged mission critical IT systems and the peripheral IT infrastructure to resume business operations post unplanned outage.

Why such a plan is critical?

Disaster occurrences are unpredictable and the financial impact to the business will vary in magnitude. The disaster can cause direct revenue loss and loss of indirect factors such as productivity loss / loss of customer confidence / impact on brand equity to the business organization. So it is essential for enterprises to have a Disaster Recovery Plan in place at all times.

Background

Treasury Department is the government agency of St. Kitts and Nevis. The agency has deployed a number of SQL Server instances spread out over different locations in Treasury and Customs, They having also planned to create another instance to other locations.

The main problem they wanted to resolve was the high availability of data critical to their main application. They engaged with Lelogix Software Pvt. Ltd. to help in the design of an architecture best fit for their needs, budget, expectations and skill set.

Stakeholders

Treasury Department, Ministry of Finance, St Kitts & Nevis.



Disaster Recovery Challenge

In today's enterprise environment, a disaster-recovery plan isn't just something that's nice to have—it's more crucial than ever. A business-continuity strategy must be formulated to ensure that when a disruptive event takes place—be it a service interruption, inclement weather or any other outage—the company can sustain its usual processes.

Creating an effective disaster-recovery plan isn't without its fair share of challenges. Unless every essential aspect is factored into the strategy, the enterprise will likely find the plan lacking when it comes time to activate it. Therefore, pinpointing and addressing these obstacles ahead of time is a critical part of a successful disaster-recovery strategy.

Following are basic challenges for Business Continuity :

- Safeguarding data in case unforeseen events.
- Faster recovery without data loss.
- Secured access to important and sensitive data.
- Tracking of changes, access and creation of data by personnel.

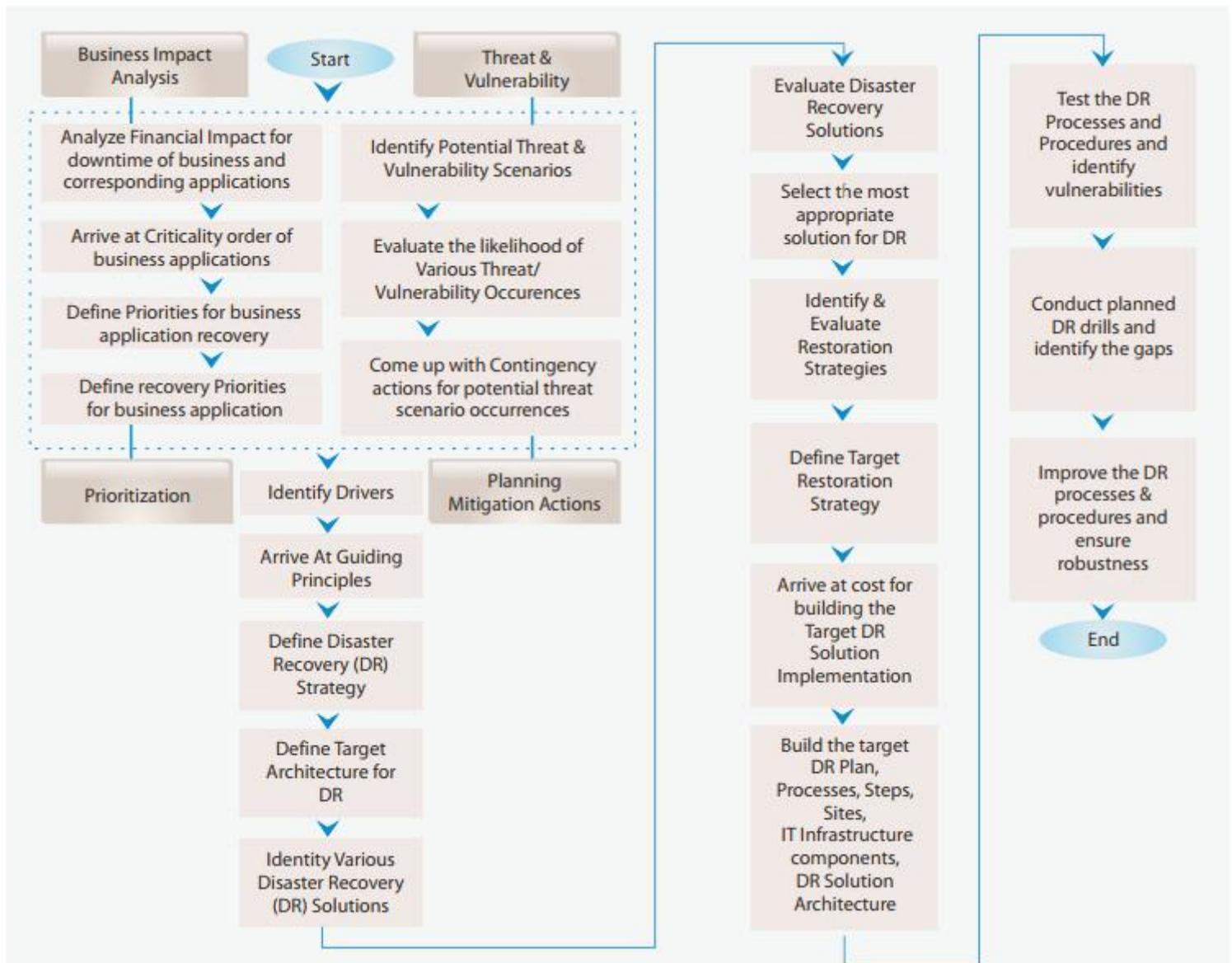
Solutions of Underline Challenges

In addition to the obstacles illuminated by the study, Lelogix's Team also noted several other issues with companies' disaster-recovery strategies:

- They may not have a disaster-recovery plan in place at all.
- The current plan is incorrect or unreliable.
- The plan includes unnecessary technology.
- The plan hasn't been effectively tested.
- The plan doesn't include sufficient information management regulations.

A Comprehensive Approach to Disaster Recovery Planning :

The essential steps involved in Lelogix' approach for arriving at the target disaster recovery plan are illustrated in the flowchart below :



Implementation & Major Work Involved

- ▶ Envision Current Infrastructure
- ▶ Management Awareness
 - Identify Possible Disaster Scenarios
 - Build Management Awareness
 - Obtain Management Sign- Off and Funding
- ▶ Resiliency and Backup Services
- ▶ Analyze High Level View of Their Original Database Topology
- ▶ Disaster Recover Planning Process
 - Establish a Planning Group
 - Perform Risk Assessments and Audits
 - Establish Priorities for Your Network and Applications
 - Develop Resiliency Design and Recovery Strategy
 - Prepare Up- to- Date Inventory and Documentation of the Plan
 - Develop Verification Criteria and Procedures
 - Implementation

Achievements & Benefits

Implement a system for protecting and ensuring data safety include the following :

- a) Use of a system that is able to replicate your data offsite thus enabling access at all times.
 - b) Backups that are automatically transferred or copied to offsite disks
 - c) Use of tapes for backup which are then transferred off site regularly.
 - d) Replicating data to off-site locations
- Business continuity solutions help maintain employee productivity and a business's ability to generate revenue
 - Backup and disaster recovery solutions help preserve a company's reputation with customers and partners.
 - Business continuity solutions help prevents companies from losing business to the competition.
 - Backup and disaster recovery helps ensure compliance with industry regulations.

Best Practices

- Create management awareness campaigns to obtain buy-in from senior management for building a disaster recovery plan.
- Include people and create a cross functional team with subject matter experts from different groups such as application business analysts, developers, system programmers, network specialists, infrastructure specialists, database administrators and data recovery specialists etc.
- Prepare comprehensive inventory of IT components and documentation of the disaster. recovery plan which also includes people roles, action sequences, responsibilities, organization structure, governance structure and escalation procedures.
- Develop key performance indicators and the mechanism to capture the metrics in order to measure the success of disaster recovery plan and processes.
- Develop robust verification mechanism and criteria for the disaster recovery plan.
- Test and verify the implementation of disaster recovery plan and processes to identify the process gaps and provide improvement measures.
- Prepare the training artifacts for disaster recovery and impart training for the cross-functional disaster recovery team.
- Document the challenges and solution workaround resolutions adopted to fix the issues during the planned disaster recovery exercises.



Why Lelogix ?

Low Costs

Onsite/ Offshore delivery model

Provides End to End Solution

Experienced Resources

Production Support & Enhancements

Help you to get Software Licenses

Help you to get Hardware

One shop for all your worries

For any Query, please visit www.lelogix.com

The information contained in this document is proprietary.

©2017 Lelogix, All rights reserved.

