Organisation of Caribbean Utility Regulators (OOCUR) 4th Annual Conference

Disaster Recovery Planning from a Regulatory Standpoint

Martin Haynes, Information Technology Manager
Regulated Industries Commission, Port of Spain
Trinidad and Tobago

OOCUR
ORGANISATION OF CARIBBEAN UTILITY REGULATORS

REGULATED INDUSTRIES COMMISSION

Topics for Discussion

- *Objective*
- *What is Disaster Recovery (DR)?*
- *Typical Approaches to DR*
- *Alternative Approaches to DR*
- *Where to Start?*
- *DR Plan*
- *Specific DR Planning*
- *Resumption Phase*
- *Restoration Phase*
- *Conclusion*

Objective

- The sole objective of Disaster Recovery is to

  enable an organisation to survive a disaster

  while

  Restoring the organisation business to normal operations

What is Disaster Recovery?

- "**Systems**" include both hardware and software.
- "**Data**" includes true data, log files and audit information, as well as "business knowledge" (such as procedures and business rules).
- "**Infrastructure**" includes phones, office space, remote access, intranets, websites, firewalls, communication devices etc.
- "**Business Operations**" are the things that your business does on a daily basis to generate revenue or improve efficiency and productivity.

Typical Approaches to DR

- **"We will just restore from backups"**
  - Where will the restore occur?
  - Are you sure the backups are good?
  - Will the data from separate systems be in sync?
  - What about offsite backups that are older?
  - Will the equipment be compatible?
  - How long will restoration take?
  - What about remote access, network bandwidth, data security?
  - What about *Running the Business*?

Typical Approaches to DR

- **DR Facilities & Service Providers**
  - Cost is “fixed” over length of the contract
  - The cost for testing may be extra
  - Contracts may lack absolute guarantees and/or service level agreements (SLAs)
  - Hardware configuration issues common
  - Availability issues may occur
  - Possible Bandwidth / Accessibility issues
  - Are they committed to your success?

Alternative Approaches to DR

- **Cold site** has electricity, A/C and phone, needs the most work and time, needs to acquire all equipment and is the least cost to setup.
- **Warm site** has all utilities, has computer hardware and software and data needs to be loaded and updated, some work required. Uptime 12 - 24 hrs.

- **Hot site** has all the capabilities of the warm site extremely expensive, it's a replica of the primary site. Uptime – real time.
- **Mobile site** is a mobile unit which has features of cold, warm or hot site.

Where to Start?

Planning

- **Create a DR Team**
  - Executive Sponsor
  - DR Coordinator
  - Team Leads and/or Members
  - Need to define both primary and backup contacts for each team position. The goal is to not have any person become a “Single Point of Failure”

Requirements

- **Identify Business Requirements**
  - Requirements are different than Goals!
  - Identify functional areas to be recovered (for example: locations, Departments, specific functionality)
  - Categorize those systems into Tiers
    1. Recover ASAP - within hours, 12-24
    2. Recover within days or weeks
    3. Recover within a month or more

Requirements

- **Identify Business Requirements (continued)**
  - Define the Recovery Time Objective (RTO). This is the goal for having the Tier1 systems operational.
  - Define the Recovery Point Objective (RPO). This states how much data can be lost based on time from the point of failure going backwards.
  - Set expectations based on this common understanding of the business goals!

Why Risk ?

Types of External Risk

- **Identify & Categorize Risk**
  - What is the most likely to occur?
    - Fire?
    - Natural Disasters such as an earthquake, flood, super tornado or hurricane?
    - Loss of infrastructure (power, network, facilities)
    - Terrorism?, Hackers?, Other “evil”?
  - Look at the probability and cost of each type of disaster, determine the “business adjusted risk” and then plan accordingly.

Types of Operational Risk

- Key Risks
  - IT systems and process failures
  - Internal Fraud
  - Natural disasters
  - Failure of utilities
  - Change in regulatory regime
  - Engineering Failures
- Risk Mitigating Strategies
- Back up tapes/internal controls
- Limits/Internal Controls
- DRPs/Insurance
- Generators/Remote Sites
- Keeping abreast of developments

Risk Assessment and Business Impact Analysis

- What am I trying to protect? (system inventory and definition)
- What am I trying to protect them from? (vulnerability and threat assessment)
- What controls are currently in place or needed to prevent or minimize the effects of potential loss? (evaluation of controls)
- How much am I willing to spend on those controls? (decision)
- Is the money I am spending effective? (communication and monitoring)

Risk Assessment and Business Impact Analysis

- Before you begin the ranking process, determine what criteria to use. Generally, criteria are split between quantitative and qualitative. Quantitative losses can be expressed as a number, such as an annualized loss exposure (ALE). The simplest ALE equation is shown in below.

A simple ALE equation

1. (R)isk = f x E :
2. (r)isk = f x e
3. B = R – r – c
4. B = f x (E – e) – c

f - Frequency

E – Exposure without control

e – Exposure with control

B - Benefit

c – Cost of maintaining control

Critical Systems

- **Identify Critical Systems**
  - Key processes and business applications
  - Dependencies and interaction with/on other network systems
  - Manual processes
  - Are there any business or legal requirements for this system (FOIA, ISO 17799, etc.)?

    If so you need to ensure compliance on an ongoing basis!

Points of Failure

- **Identify Single Points of Failure**
  - The goal is to mitigate unnecessary risk, *within reason*
    - Identify Single Point of Failure (SPOF) items
    - Estimate the Probability of Failure
    - Estimate the Number of Incidents per year
    - Estimate the Cost per Failure and the Annualized Loss Expectancy (ALE)
    - Compare the Cost of Mitigation to the ALE

Personnel

- **Identify Key Personnel**
  - The DR Team!
  - Identify Roles and Responsibilities
  - Associate Names with the Roles
  - Have a clear policy defined regarding who has authority to do what:
    - For example, who can declare a disaster and under what circumstances?

The Disaster Recovery Plan

Disaster Recovery Plan

- **Computer Systems Documentation**
  - **Systems overview and roles and responsibilities of the department**
  - **Systems components and basic setup**
  - **Systems Management**
  - **Operational Network Procedures**
  - **Troubleshooting and maintenance**
  - **Back up and Data Restoration**

Disaster Recovery Plan

- Business Resumption Plan
  - Business Impact analysis
  - Potential workaround & solutions
  - Damage Assessment Strategy
  - Recovery strategy
  - Recovery team
  - Recovery of server System
- Testing Strategy
  - Disaster scenarios,
  - Objectives and assumptions
  - Test parameters and procedures

Disaster Recovery Plan Details

- Planning and Configuration
- Detailed Recovery Procedures
- Detailed Test Plans
- Detailed Security Plan
- Plan to Restore Operations
- Post-test clean-up
- Standard Method to Define Success
- Standard Review Process
- Test, Validate, and Refine

Disaster Recovery Plan

- **Planning and Configuration**
  - Just because it looks impressive in MS Project or Primavera doesn't make it a good or valid plan!
  - Shows detail configuration of critical systems
  - Shows dependencies, helps identify overlap
  - For most sites the plan should be at a higher level,pointing to detailed recovery procedures

Disaster Recovery Plan

- **Detailed Recovery Procedures**
  - Design the procedure to be used by someone who is not an expert with the system being recovered
  - Provide specific commands and representative output from those commands
  - Provide check boxes and an area to write in time started / completed and comments
  - Cross-training provides both depth of coverage and validation of the process

Disaster Recovery Plan

- **Detailed Recovery Procedures** - Continued
  - Provide troubleshooting information
    - Decision trees work well for this
    - Anticipate typical problems and proactively provide information to resolve the problem
  - Provide alternate means of recovery
    - Anticipate the worst (and plan accordingly) while hoping for the best

Disaster Recovery Plan

- **Detailed Recovery Procedures** - Continued
  - Provide Vendor Support information
    - Technical Support contact information
    - License numbers
    - Sales person contact information – used to escalate issues if necessary

Disaster Recovery Plan

- **Detailed Test Plans**
  - Need a way to validate that critical systems have been fully and properly recovered
  - Need to validate external access, access to dependent systems, data feeds, etc.
  - Will ideally provide the means to validate the accuracy of the data
  - Provide basic performance validation

Disaster Recovery Plan

- **Detailed Security Plan**
  - What needs to be secured and why?
  - Can secure and non-secure data “co-mingle” on a network?
  - Physical security and safety issues should be addressed
  - By what means will people be accessing these systems? Will the connection be secure?
  - Use of production passwords may be a concern at third-party recovery test sites

Disaster Recovery Plan

- **Plan to Restore Operations**
  - In a true disaster, the recovery site may be used for weeks or even months
  - Eventually the original operational site will be restored or rebuilt, at which time the recovery site will become unnecessary (or at least secondary)
  - Typically a “Reverse DRP” is used to restore the systems to their final production location

Disaster Recovery Plan

- **Post-test clean-up**
  - Remember, the restored systems are now de facto production systems
  - The systems should be thoroughly “scrubbed” once testing has been completed
  - Failure to do that may result in someone or some other company having access to your production data!

Disaster Recovery Plan

- **Standard Method to Define Success**
  - We use a “Critical Success Factors” spreadsheet that uses weighted values assigned to various systems, functionality, and dependencies
  - Provides a way to demonstrate success and point out areas for improvement
  - Provides a means of tracking both progress and complexity of the overall plan
  - It also highlights flaws and problems due to its use of weighted values and dependencies

Disaster Recovery Plan

- **Standard Review Process**
  - Identify what went right and what went wrong – identify “lessons learned”
  - Determine why things went wrong and improve the process
  - Look for other opportunities for improvement
  - Efficiency
  - Integrity
  - Automation

Disaster Recovery Plan

- **Test, Validate, and Refine**
  - Requires full scale recovery tests on a regular basis
  - Staff should be rotated as a means to verify the accuracy and ease of use of the recovery procedures
  - Failure to do this will result in providing a false sense of security!

Specific
Disaster Recovery Planning

Specific DR Planning

- Identify and document, **Operating System, Hardware System, Network, Operational procedures** and **Database System**

  Specific Configuration Information

- Use operational procedures to restore **Operating System, Hardware System, Network,** and **Database System**

  Specific Configuration Information

Specific DR Planning

- Identify and document Windows **OS** specific information
  - OS parameters
  - User & Group, info from Active Directory
  - OS version & patches applied
    - It is important to know how to rebuild the system.
    - Have proper and detailed documentation on every system configuration

Specific DR Planning

- **Prerequisite Step – Restore Server (Mirror Production Configuration)**
  - User Accounts and Groups
  - Filesystems
    - Size
    - Ownership
    - paths
  - Any critical directories and files
  - Specific files that have been customized
  - OS patches

Specific DR Planning

- **Restoring the OS Installation**
  - OS Backup, determine if its good
    - Also helps minimize problems related to OS files
  - Be prepared to reinstall OS
    - Implies that both the installation media and the patch media (for the patch version used in production) is readily available

Specific DR Planning

- **Restoring the Databases**
  - Rollforward DB ideal
    - Point in time recovery requires restore points and
    - Recovery up to the point of failure requires the transaction log file (SANs really helps here)
  - OS Backups & Reload from unloads are a last resort
  - Know your RPO! (Recovery Point Objective)

Resumption Phase

Resumption Phase

- **Validating the Environment**
  - Does all required products work?
  - Does Network connections work?
  - Are there any unusual errors in the event.log file?
  - Do all standard tools and facilities work?
  - Is performance consistent with what you are familiar with?
  - Test to make sure that “restricted access” really is!

Resumption Phase

- **Safeguarding the Environment**
  - This is now production – treat it as such!
  - Immediately checkpoint the database(s) and enable journaling
  - Plan for routine care and maintenance of the environment
    - Checkpoints
    - Table modifications

Restoration Phase

Restoration Phase

- **Best Practices**
  - Keep multiple copies of installation and patch media offsite or in a vault (but readily available)
  - Collect important configuration information daily or weekly and save copies offsite
  - Validate your checkpoints on a regular basis
  - Provide means of validating key data at any point of time (within reason)

Restoration Phase

- **Common Problems**
  - OS Licensing
  - OS kernel parameters and/or patches different
  - Paths not the same
  - "hostname" is different (can be corrected, but it is far easier to make certain it is the same)
  - Net password and node problems
    - Use hostnames instead of IP addresses when defining node entries to minimize problems

Conclusion

- It is important to understand the true purpose of a DRP by defining specific requirements, to determine what constitutes success.
- Develop a comprehensive plan to ensure success.
- The plan will need to be updated, refined over time as your business environment changes.
- Disaster Recovery Planning can be challenging and a very expensive undertaking, but it is one that could literally determine the future of your company after a disaster.


Thank You