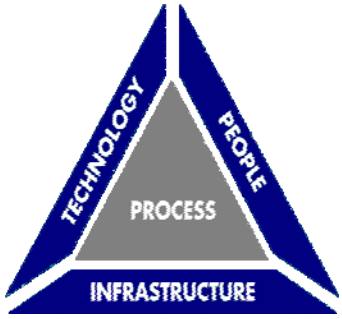

Disaster Recovery Planning Overview

January 1,
2011

Presented by: BTCG, LLC

Email: info@BTCGllc.com

Phone: (920) 836-3456

Copyright © 2007 - 2011 – Business Technology Consulting Group, LLC

Disaster Recovery Planning (DRP)

Disaster recovery planning is the planning, process, policies and procedures that are related to preparing for the recovery from outages in the technology infrastructure that is critical to an organization after a natural or manmade disaster. DRP is a subset of business continuity planning. From an Information Technology (IT) perspective, DRP is mainly focused on recovering systems, applications, data, hardware, communications (telephones and networks) and other IT infrastructure.

Business Continuity Planning (BCP) refers to the DRP as part of the overall plan and also includes planning for non-IT related aspects such as key personnel, key business processes, functions, facilities, crisis communication and the protection of assets and reputation. The focus of this document is on Disaster Recovery Planning as it pertains to technology infrastructure.

Why it is needed

Information Technology continues to become more integrated into the fabric of business and therefore the infrastructure that is the platform for this technology has become more critical to virtually all businesses today. In this new economy, your competition is: "Just around the global corner"™ and it is also becoming more common to operate businesses on a 24x7 basis, often on using the web for order taking and fulfillment. Finally, an increasing number of very visible and Key Business Processes rely on your IT Infrastructure. It is estimated that most large companies spend about 3% of their IT budget on disaster recovery planning, with the aim of avoiding larger losses in the event that the business cannot continue to function due to loss of IT infrastructure and data. The statistical survivability of companies that had a major business data loss follows:

- 43% never reopen
- 51% close within two years
- Only 6% will survive long-term.

Copyright © 2007 - 2011 – Business Technology Consulting Group, LLC

Disaster Causes

Disasters can be classified in two causes: Natural and Man Made (for the purposes of this document please note that outages caused by technology staff errors are not included as disaster events)

1) Natural Disasters- Preventing a natural disaster is very difficult, but it is possible to take precautions to eliminate or reduce their impact on you business.

- Natural Disasters
  - ☐ Hurricanes/Typhoons
  - ☐ Floods
  - ☐ Fires
  - ☐ Tsunamis
  - ☐ Earthquakes
  - ☐ Blizzards
  - ☐ Droughts
  - ☐ Tornadoes
  - ☐ Epidemics

2) Man Made Disasters- These events can also cause significant down time and consequent business impact. Again, it is possible to take prudent precautions to protect and insure your business operations.

- Man Made Disruptions
  - ☐ Chemical Spills
  - ☐ Blackouts / Facility Failures
  - ☐ War / Terrorism / Riots
  - ☐ Strikes
  - ☐ Security Breach
  - ☐ Denial of Service Attacks
  - ☐ Virus & Spyware

Copyright © 2007 - 2011 – Business Technology Consulting Group, LLC

Guidelines in creating DRP

1. Identify the scope limits on your disaster recovery plan. By not placing initial limits on the effort, your organization may fall prey to a continually growing project, or worse, attempt to protect every application and feature against every possible disaster. While these may be laudable objectives, the entire effort could collapse under its own weight, in term of complexity and/or cost, with no tangible benefits. By establishing the scope of the initial project you provide an idea for limitations and boundaries of the plan. The scope should also include the reports from a risk analysis and audit results.
2. Conduct a **business impact analysis (BIA)**.
   Business impact analysis is the study and assessment of financial risk to your organization and business loss that could result from a disaster event such an interruption of key business services or processes.
3. The support of executive management is a mandatory step in completing a successful DRP. Their authorization to expend resources in this area is necessary and it demonstrates a financial commitment and sends a strong prioritization message to the business and technology teams.
4. Designated DR personnel must fully understand their role and what actions as required of them in an actual event or a test of the DRP to make it a success. Furthermore, each participant should actively provide feedback during test on plan shortfalls and assist in developing improvements in order to continuously adapt and improve the DRP for their individual department.
5. The DRP project team must be responsible for the implementation of the plan.
6. Initial and recurring employee training on the DRP is essential in order for it to be functional.
7. Initial and recurring testing of the plan is also an essential element to make a /DRP a success.

Specifying Data Loss and Downtime

Recovery Point Objective (RPO) is the amount of data loss, (measured in time) that is "acceptable" to the business in a disaster event. The RPO is the point in time to which you must recover data as per the agreement with the business. Example: If the RPO for a specific system/service is 4 hours, yet the time it takes to get the data back into production is 9 hours, the RPO for the specific system/service is still 4 hours. Based on this RPO, the data must be restored to within 4 hours of the disaster.

Example: If there is a complete replication at 5:00am and the system dies at 8:59am without a new replication, the loss of the data written between 5:00am and 8:59am will not be recovered. This amount of time data has been lost has been deemed acceptable the RPO deems 4 hours of loss as acceptable. This is the case even if it takes an additional 5 hours to get the site back into production. The production will continue from the point in time of 5:00am. All data in between will have to be manually recovered through other means.

The RPO in conjunction with the Recovery Time Objective (RTO) is the basis on which data protection strategy is developed.

Copyright © 2007 - 2011 – Business Technology Consulting Group, LLC

Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points. RTO is established during the Business Impact Analysis (BIA) by the owner of that process. It should be noted that the RTO attaches to the business process and not the resources required supporting the process.

The RTO and the results of the BIA in its entirety provide the basis for identifying and analyzing viable strategies for inclusion in the DR plan. Viable strategy options would include any which would enable resumption of a business process in a time frame at or near the RTO. This would include alternate or manual workaround procedures and would not necessarily require computer systems to meet the RTO.

Note that RTO is an objective, not mandate. In reality, a strategy is sometimes selected that will not meet the RTO due to cost or complexity. In this instance the RTO will not be met but should still remain an *objective* of future strategy revision. It is important that gaps between DRP capabilities and RPO and RTO be fully documented and understood by the executive team.

Strategies and Tactics

Prior to selecting a disaster recovery strategy, a disaster recovery planner should refer to their organization's business continuity plan, if one exits, which should indicate the key metrics of recovery point objective (RPO) and recovery time objective (RTO) for various business processes (such as the process to run payroll, generate an order, etc). If a Business Continuity Plan is not in place, then the metrics must be agreed to by the business process owner. Either way, the metrics specified for the business processes must still be mapped to the underlying IT systems and infrastructure that support those processes.

Once the RTO and RPO metrics have been mapped to IT infrastructure, the DR planner can determine the most suitable recovery strategy for each system. An important note here however is that the business ultimately sets the IT budget and therefore the RTO and RPO metrics need to fit with the available budget. While most business unit heads would like zero data loss and zero time loss, the cost associated with that level of protection may make the desired high availability solutions impractical.

The following are some approaches to mitigating risks posed by disasters:

- Preventive Strategy – This strategy employs one or more precautionary tactics designed to prevent and/or minimize interruptions from occurring. **Below is a small sample of examples of deployment measures: (Many additional tactics are available)**
    - System and Data protection Facilities Protection
        - Backups made to tape and sent off-site at regular intervals.
        - High availability systems which keep both the data and system replicated off-site, enabling continuous access to systems and data

Copyright © 2007 - 2011 – Business Technology Consulting Group, LLC

- Facilities Protection
  - Building and/or equipment surge protection to eliminate or reduce the damage caused by power spikes or lightning strikes
  - Backup generators to minimize the effects of a medium length power outage
  - Uninterruptible power supply (UPS) to minimize the effects of a short power failure
  - Fire preventions — alarms, fire extinguishers, fire suppression systems to contain and control fires.
  - Dual building egress points for telecommunications and electrical services.
  - Contract with hosting facilities to provide alternative data center locations and/or hardened facilities within which to house your critical production and/or DRP systems.
  - Provide redundant Air Conditioning and electrical systems to power the critical
- Security Protection
  - Key card access to restricted areas
  - Data classification policy and procedures
  - Properly configured and monitored firewalls
  - Conduct security risk assessments and properly mitigate vulnerabilities.
- People
  - Cross train staff to provide emergency or transition support and avoid single points of failure.
  - Provide travel, expense and housing arrangements for the event response team.
  - Monitor news sources to determine if disaster or utility stoppage events are impending.

- Corrective Strategy – This strategy focuses on providing recovery tactics aimed at correcting or restoring the system after disaster or event.
  - System and Data protection
    - Create and exercise processes and procedures designed to expedite the return to normal service state of systems
    - Restore data and systems from backup tapes stored off site.
    - Redirect the user community to alternative data centers and systems during an event.
    - Contract with manufacturers and third party support providers to provide on-site and/or remote/telephone support and hardware as required.
    - Manually or mechanically enter data that was recorded using an alternate process during the disaster event.
  - Facility protection
    - Contact with professional service providers to repair facility systems to meet the service levels required by the business.
  - Security Protection
    - Create security response policies and procedures to rapidly and appropriately react to events

Copyright © 2007 - 2011 – Business Technology Consulting Group, LLC

- People
  - Authorize travel and expenses for the event recovery team.
  - Contract with telecommunication service providers to reroute critical business links, phone numbers, email traffic to pre-designated alternative facilities.
  - Prepare and disseminate event status updates to the employees, client and vendors.

In Summary

A Disaster Recovery Plan requires the participation of both the business and the technology teams. The technology team should create and implement all of the appropriate policies and procedures needed to avoid system down time that may be created by the IT department itself as this is the leading statistical cause of data loss events. A business impact analysis should be accomplished in order to provide the business' insight into system criticality to the technology team. The technology team should design and implement solutions that meet the service level needs of each business requirement. Training and testing of the plan is a continuous requirement to ensure that downtime and business impact is minimized. Since businesses are rarely static, the entire organization should be aware of the current DRP and consider how changes to business processes or function may require adjustments to the Business Continuity plan which may in turn require changes to the Disaster Recovery Plans. These potential changes to the needs should be brought to the attention of the DRP team as soon as they appear so that they may be evaluated and if necessary, addressed. Finally, Disaster Recover Planning reviews and DRP testing should become a part of the organization's culture and considered a vital part of the organization's survivability.

Contact BTCG for more information at info@BTCGllc.com or call (920) 836-3456

Copyright © 2007 - 2011 – Business Technology Consulting Group, LLC