CMB Disaster Recovery Project Overview

The overall goal of this project is to provide the City of Miami Beach with a disaster recovery strategy that addresses the business requirements of all City departments in the event of a disaster; also, which is in line with the City strategic plan and/or vision. Prior to this project, the concept of disaster recovery as it pertains to technology services which will be referred to as "DR" going forward, was limited to recovery off of backup tapes. This strategy did not take into consideration a scenario that involved permanently losing a facility or technology hardware. This method of recovery in the IT department's opinion was not a satisfactory enterprise strategy for the City, as it basically translated to an enormous amount of downtime during a worst case scenario disaster, where loss of the core datacenter could occur. Seeing as the City of Miami Beach is essentially a barrier island this scenario is not too farfetched, as predictive models show that a direct strike by a CAT5 weather event will cause major damage to the City. Although, weather events are not the only type of disaster that could present itself, with respect to the City's geographical location, it is the worst case scenario type of disaster that could present itself. IT best practices for disaster recovery planning purposes, will always establish a strategy that will address the worst case scenario for the organization.

It was here that the IT department drew on the experience of its current management team; in order to expedite the research and evaluation phases of the project. There are many approaches that can be taken with respect to coordinating this kind of an effort; however, the best and most successful approach is to have a 3rd party conduct a formal BIA (*Business Impact Analysis)*. Essentially, a BIA is a risk assessment tool that considers a range of possible disasters, including natural, technical, human and societal threats. It is important that each functional area of the organization be analyzed to determine the potential consequences and impact associated with several disaster scenarios. The BIA is basically what drives the project in its entirety from its inception, as it helps the IT department manage the scope and avoid scope creep during implementation, by having all City departments agree to what is and isn't critical and/or what is and isn't required from a logistics perspective from the very beginning. Additionally, it allows one to manage expectations effectively as the DR strategy is executed. It is also important that during the risk assessment process, the safety of critical documents and vital records be assessed. It is important to assess the impacts and consequences resulting from loss of information and services. The BIA that conducted at the City was very instrumental to the formulation of a proper DR strategy.

CMB Business Impact Analysis

Executive Overview

The purpose of the CMB BIA has three main goals.

1. Verify the Recovery Time (RTO) and Recovery Point (RPO) requirements of the CMB business / governing functions,

2. Assess the recoverability of the CMB Information Technology systems (CMB IT) supporting the city's business and governing functions

3. Provide high-level IT strategies and recommendations to improve the current IT Disaster Recovery / Business Continuity Planning.

The mission of the Information Technology Department is to provide tools that enhance the CMB's ability to deliver world-class service to the City's residents and visitors by helping the City satisfy its customers' needs for creative solutions.

In line with the City's Strategic Plan and Goals relating to the use of Technology as well as the current philosophy of Performance Based Management, the following are examples of Key Performance Outcomes:

- Improve the effectiveness and efficiency of City processes/procedures and enhance employee performance
- Deliver hardware and software systems that meet/anticipate the City's needs, are cost-effective, are timely, and are supportable
- Maximize the City's return on investment in technical assets
- Lower the barriers between City agencies and City residents

Disaster Recovery Planning for the IT systems supporting CMB is also a Key Performance indicator. The IT Department has responsibility for the information technology supporting CMB business and governmental functions. Therefore, it is incumbent upon CMB IT to implement IT Disaster Recovery strategies that meet the city's requirements for operational continuity.

Recovery Time and Recovery Point Objectives for the systems / applications that are supported by CMB IT were defined during a series of Recovery Objectives Validation Workshops, conducted by Mainline Disaster Recovery Services. In FY0607, the City conducted the ROV Workshops, and reviewed the processes and procedures that are utilized in the current IT production environment, backup and recovery procedures, and vital records processes employed to protect CMB's critical data. Afterwards, CMB's potential recoverability was measured against the Recovery Time Objective (RTO) / Recovery Point Objective (RPO) requirements that were defined during the ROV Workshop. The Recovery Time Objectives agreed upon in the ROV Workshop for the various systems that reside in the CMB Data Center are in a range between 8 hours and 120 hours.

The review determined that it was not currently possible for CMB to recover the critical applications in the time-frames required. It likely would have taken several weeks to completely recover from a total loss of the CMB IT infrastructure located in the CMB PD Datacenter. This is primarily due to the lack of a pre-determined, fully implemented, and tested recovery strategy that ensured a place to relocate, and the available resources to enact recovery during an event where the datacenter is destroyed and/or inaccessible for a prolonged period of time. Without pre-planning, it would likely take weeks to reestablish critical systems. To date, CMB IT and CMB Executive management has shown exceptional leadership by locating and planning for LAN / WAN redundant connectivity inclusive of the Primary Data Center, NAP, City Hall, and EOC. This planning and leadership has provided a solid base on which CMB can establish an IT Disaster Recovery / Business Continuity strategy that will meet the city's requirements for operational continuity.

Solution / Plan / Proposal

After weighing the various platform and site recovery strategies that we had at our disposal, we eventually decided on adopting a mixed strategy for the City of Miami Beach. Fortunately for the City of Miami Beach, just 6 miles away from the City was a hardened co-location facility that could be leveraged as part of the solution. The co-location facility is a CAT5 rated, with various levels of redundancy for environmental (power, A/C, etc.) and communications. The co-location facility is host to the Federal government's USAF Southern Command *(previously located in Panama)*, as well as numerous other organizations such as Miami-Dade County and CBS sports to name a few. In short, although the facility was within the geographic region of the City, the facility was more than adequate to meet the City's needs from a DR perspective. Typically Co-Location facilities are selected way outside of the geographic region of the organization; however, based on the level of hardening we did not feel this would be an issue. After deciding on our co-location facility, we determined that due to its close proximity to the City that it would really not be cost-effective to establish duplicate systems *(for all Hot and Warm Systems)* and or overcomplicate the environment with geographically clustered systems if we could avoid it, as a result, we decided to make the Co-Lo facility our actual Production facility for all critical City systems. Assuming that we utilized managed devices for power and system console (Session 0) access, all system maintenance could be handled remotely without the need for being physically in front of the equipment. Realistically, the only real physical interaction would be required in the event of a physical hardware type problem; also, in the event that were to occur, an administrator could be on-site at the co-location facility within (15-20) minutes.

The City's existing datacenter infrastructure would continue to be utilized; however, it would be solely for the purposes of housing systems that are considered to be Development and/or Sandboxes, which based on our DR BIA results, could be recovered using traditional DR recovery strategies as required. Additionally, these systems could potentially be recovered using a virtual type VMware server environment(s) if necessary, which would further speed the recovery process and lessen the amount of physical hardware required to do so. In addition to critical city systems, we also reviewed our existing Internet Gateway requirements and telecommunications / VOIP / voicemail requirements and decided to not only move production systems to the co-location facility, but also to move our main Internet head end and voicemail system to their as well. Consequently, this also led to establishing a 3rd VOIP switch at the facility that would handle all primary call routing for the City. This basically would allow the City of Miami Beach to continue to receive calls and voicemail messages from residents, business, etc. *(during and after a disaster)*, even if worst case scenario all City facilities are knocked out by a weather event. Once the end user recovery solutions are enacted, those messages would be available for City personnel. To date all phases of this project have been completed successfully due to the hard work and efforts of CMB IT staff and the support of CMB Executive staff. Future needs that have been discussed by IT management and Executive Staff is instituting Tertiary data replication to an offsite location as an additional measure of data protection; also, establishing a formalized end user recovery strategy.

DR / BCS Strategy

Recommended IT Recovery Strategy:

Primary Data Center ←— Data Replication —→ **COLO**

Tape Backup (Rotate Offsite)

Cold Systems

Systems identified as having a RTO (Recovery Time Objective) of Greater than 72 hours to 1 Week are considered Cold Systems and recoverable using traditional backup strategies.

Strategy adopted to meet City needs could be categorized as a Mirrored / Co-Location Strategy.

Hot and Warm Systems

Systems identified as having a RTO (Recovery Time Objective) of 0 – 72 hours are considered Hot and Warm systems; as a result, were moved to the co-location facility to allow for both Business Continuity and Disaster Recovery. Moving the systems to the hardened co-location facility was the most cost-effective solution, requiring the least amount of system duplication and maintenance.