Business/IT Continuity Management

Pradeep K Juneja, FIETE
Independent Technology Consultant, 2-B, DDA flats, Masjid Moth, New Delhi-110048, India
pkjuneja@gmail.com

Abstract -- **9/11 changed the mindset of business and IT people throughout the world. Irrespective of the size of any company, people started giving due consideration to the business and IT continuity. Business continuity management (BCM) and contingency planning are essential and unavoidable tasks. There is always a tussle between the business and IT management as to whose responsibility is to plan and implement the business continuity. Both are equally important and must go hand in hand to achieve the business continuity. They have to look into their respective areas to achieve it. For example, the IT team can ensure the availability of the IT systems but if the business people have not planned for how to use those systems from a Disaster Recovery Centre (DRC) then the whole purpose of the business continuity is lost. The creation of a sound continuity and contingency plan is a complex job involving a number of stages and discrete activities.**

Initially it is necessary to understand the underlying risks and the potential impacts of a disaster. These are the building blocks upon which sensible business continuity plan (BCP) or disaster recovery (DR) plan should be built and the plan must be implemented. There are the maintenance and testing phases, to ensure that the plan remains current. The plan should be audited and then put to practice. This is just a snapshot of the business continuity, its important components, need, how to go about it and some other important aspects. While arriving at a final business continuity plan for an organisation, a detailed study is required to assess the current preparedness, finding the gaps, implementing the desired customised solution, maintaining it and to carry out constant reviews/modifications in order to keep it current and ready to use.

Keywords: IT Management, Network Recovery, Business continuity planning, *Business impact analysis,*

I. INTRODUCTION

THE first step in a sound business continuity planning process is to consider the potential impacts of each type of disaster or event. This is critical - one cannot properly plan for a disaster recovery if one has little idea of the likely impacts on their business/organisation of the different scenarios.

Business impact analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. The business impact analysis is intended to understand the degree of potential loss (and various other unwanted effects), which could occur. This will cover not only just the direct financial loss, but also other issues, such as reputation damage, regulatory effects, etc.

High Availability (Zero Down time): In any enterprise IT set-up, only important equipment should be considered for high availability. Depending upon the option, Clustering, Mirroring or similar technologies should be deployed.

Continuous Availability (24*7): To achieve this, an optimum mix of Hardware, Software and processes should be looked into.

Disaster Recovery (DR): It has many factors to be considered, for example fire, flood, earthquake, terrorism, and country's telecommunication network etc. Effects of the fire can spread to a few 100 metres. Flood can impact a few kilometres. Earthquakes can impact a few cities. Terrorism/Vandalism are usually localised to an area. While planning for the business continuity, one has to decide, out of these possible events, which of these should be considered to guard against their occurrence. This helps in choosing the disaster recovery centre (DRC) location. It can be a few metres away, a few kilometres away, in a different city, in a different country in the same continent or a different country in another continent. The costs involved will have huge difference for different scenarios. That's where the role of business people comes in the picture, what do they want to guard against and at what cost. IT people will accordingly provide the solution.

II. NEED FOR THE BUSINESS CONTINUITY

Cost of downtime: Cost of downtime should be viewed as a loss of revenue. Decision makers should comprise the Business people and IT staff. The decision should be taken by answering the question: What will be the impact on business if the business systems are not available.

Planned downtime: It should be in the off-peak hours as far as possible to carry out the planned system activities, e.g. Operating System changes, Maintenance activities etc. Stakeholders should be informed about it in advance. Once the users give their nod, it should be performed. IT people usually plan it during the organisations' holidays. This is usually unnoticed by the management. Constantly working during holidays has impact on IT staff's physical health and social life. HR, business and IT Management should adequately compensate or plan job rotation for all those staff members who continuously work during the off hours.

Unplanned downtime: It is an unusual situation, which can never be planned. Some of the precautions could be exercised to avoid unplanned downtime. By carefully planning the redundancies of the equipment and processes, business can be recovered and resumed at either slow pace or with limited availability. In some cases, putting manual processes in place can lead to the reduced downtime at low cost.

Duration of downtime: Linked to the above, duration of downtime should be planned to be minimum. It can be achieved by factoring the reasons of downtime and their anticipatory solutions.

Reasons of downtime:

Security violations: A system can go down because of a process disruption, which is caused by an unauthorised access.

Data corruptions/Application Failures: Some of the common reasons could be an untested module or changes in programme, hard disk errors, power, power fluctuations, frequency changes etc.

Power outages: In order to avoid power outages, a right mix of generator/UPS should be chosen. Whenever a graceful shutdown of devices is required, UPS should meet the requirement. If the business demands continuous operation in the absence of the main power, generator should be considered. Its diesel availability should be ensured. It is recommended to have main power from different grids.

Human error: A very common cause of human error is accidentally tripping the power; say resetting the ELCB (Earth Leakage Circuit Breaker), loose power connections etc. Positioning of such devices should not be in the passage. If it is unavoidable, then these should be installed in a wall mount cabinet.

Failed upgrades: Sometimes, prima facie everything seems in order after an upgrade is carried out. When the system is subjected to full load, the problems start surfacing up.

Natural disasters: As discussed above, system outages can be due to natural disasters. Adequate BCP/DR Plan can minimise downtime arising out of such situations.

Failures: There can be many reasons for an IT set-up failure, e.g. Power; Network; Computer System; natural disasters like fire, flood etc.

Network failure: Computer Systems could be working, but if the network is down, then users may not be able to use the same. Hence, network availability has to be looked into as one of the most important components of the IT set-up. Usually, a network failure leaves more than one user out of service. Hence, network resources should be deployed in such a way that the requisite redundancy is assured.

Computer System Failure: If the main computer is down, there is a very heavy impact on the business. Users cannot do anything. This is the worst scenario in any IT set-up. Hence, adequate measures should be taken to ensure business continuity.

Signs of Downtime:

- Shrinking Backup windows: Take backup on high speed removable media.
- *Globalise Computing*: Grid computing is slowly gaining acceptability in the IT world.
- *Distributed Applications*: From the backup time viewpoint, it indirectly gives the benefit if Grid Computing as processing is distributed.
- *Server Consolidation*: It helps in consolidating the data on to a few servers. Thus backup process involves fewer drives and eases its management.

III. BCP – BUILDING BLOCKS

People: In order to have a BCP, its implementation and sustenance, it is recommended to have a dedicated BCP team comprising staff from business and IT. It should be involved in the periodic audits and simulations.

Processes: BCP team should thoroughly study the existing procedures and suggest modification or new processes as the case may be. Processes should be periodically reviewed and changed according to the prevailing situations.

Products/technology: BCP team should constantly scan the market for products and technology to improve the availability.

IV. STEPS INVOLVED IN BCP

Response: From the action viewpoint, Who, How, When, What should be clearly defined in BCP depending upon the failure.

Recovery: If the failure is already defined in the BCP, its recovery should be as per the Recovery Plan/Guideline given in the BCP. If it is a first time failure (of unknown nature), BCP team along with technical members and users should come out with a recovery mechanism.

Resume: This could be a total or partial resumption depending upon the remedial actions. An ideal method is to release the resources step-by-step so that if any device malfunctions, it should not result in a bigger failure. For example, due to power fluctuations servers are switched off. Once it is established that the power situation has improved, release a couple of

low priority servers and observe for any power fluctuation. If fluctuations were still there, one would have averted a bigger outage. If fluctuations are not there, all the servers could be resumed.

V. BUSINESS CONTINUITY STRATEGY DESIGN

The strategy for implementing the Business Continuity Planning is unique to an organisation. BCP are developed based on the potential threats faced by the organisation. Generally the BCP is geared to meet all the possible contingencies, be it operational, infrastructural or unforeseen natural calamities. An organisation's Business Continuity Management (BCM) system is strengthened by the 'Information Security Management Systems' (ISMS) initiative, which complies with the requirements of ISO 27001 standard.

BCP begins right from the requirements gathering phase. This is reinforced during the transition phase. Business Impact Analysis (BIA), Recovery Time Objective (RTO) Analysis, Recovery Point Objective (RPO) analysis and Disaster Threat Analysis are the various steps carried out while implementing the BCP Strategy.

The strategy for BCP is commensurate with the organisation's budget and the level of operations that could be scaled down in the aftermath of a disaster.

For a sound BCP there is a need to conduct surveys, talk to the users, vendors and come up with a strategy based on the analysis of a business environment.

Business Impact Analysis (BIA): Business Impact Analysis Workshop needs to be conducted to review the following:

i. Review of current operational and recovery processes for all the Applications running in the environment
ii. Review of the Data Backup and recovery procedures
iii. Review of the existing resources
iv. Review of the existing Business Processes
v. Review of the hardware and software configurations of the existing Infrastructure
vi. Review of the existing IT environment with respect to Air-conditioning, Dust Free & Humidity Free environment, Direct Sun Light Exposure
vii. Review of the existing Emergency preparedness procedures

Risk Analysis: Based on the results of BIA, there is a need to do a Risk Analysis to

i. Identify potential exposures and vulnerabilities
ii. Suggest alternatives and solutions
iii. Suggest the use of specific tools & right resources
iv. Document findings and recommendations
v. Define Preliminary Recovery Strategy
vi. Prepare, schedule and conduct a Review Session

Business Continuance Objectives- Organisations need to determine their objectives for business continuity in terms of Recovery Time objectives (RTO) and Recovery Point objectives (RPO).

i. Recovery Time Objectives (RTO)
   a. Determine how long one can afford to be without the computer systems
   b. Define how quickly there is need to restore the applications and have those fully functional again
   c. The faster the RTO requirements, the closer one moves to zero interruption in uptime and the HA (High Availability) requirements

ii. Recovery Point Objectives (RPO)
   a. Determine how much data one can afford to recreate
   b. Define the point at which the business absolutely cannot afford to lose data
   c. Points to a place in each data stream where information must be available to put the application or system back in operation
   d. The closer one comes to zero data loss and continuous real-time access and higher availability; one will require a network switchover strategy.

iii. Network Recovery Objective (NRO) – Issues related to when to decide to switchover and how long to switchover the network

Cost/Recovery Time Curve

Based on the above facts determine the Cost/Recovery Time Curve. Cost vs. RTO Recovery curve is the key to selecting the proper solution(s). Decision Making factors are:

- Feasibility of in-house DRC vs. outsourcing DR Services vis-à-vis" One time cost and recurring costs of having DR Centre
- Involvement of dedicated resources including user community
- Updates of the DR plan with respect to the changes in Business Processes/Technology
- Periodic testing of the DR plan

VI. BCP LIFECYCLE

All the aspects of a BCP/IT Continuity described above can be depicted in the form of a BCP Lifecycle (Figure 1). The BCP lifecycle process takes on many dimensions identifying all the operational attributes of a mission critical business service. The BCP lifecycle is a continuous process and revolves around the business as it changes as and when any new products and services are introduced. Failure to include any new mission critical business services into the BCP lifecycle process can result in the failure of recovering a mission critical business service. A schematic representation of BCP lifecycle is shown in Figure below:

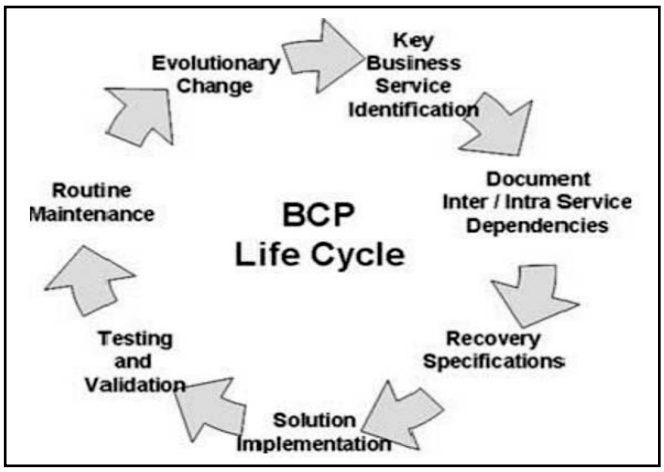

Figure 1. BCP Lifecycle

VII. BCP AUDITING AND ASSURANCE

BCP auditing and assurance is done to ensure the completeness of the business continuity plans by encouraging the use of Business Impact Assessments and Threat and Risk Assessments (TRAs) and to completely integrate with respect to the support functions and dependencies. The BIA identifies and quantifies the direct and indirect, quantitative and qualitative impacts on the critical and essential services due to disruptions and emergencies. Another control objective is to ensure that the business continuity plans should include a fully documented business continuity recovery strategy that detail steps to provide critical and essential services.

IT Resources Inventory: Each of the IT Resources, i.e. Hardware, Software is an asset of the company.

Recovery Procedures: Recovery procedures for various types of the disaster scenarios analysed in the Business Impact Analysis are written, tested and maintained. Change management control system should be adopted. If any business process change occurs or when the technology is upgraded so that the cycle is completed only when the recovery procedures associated with the change are also updated and put in place. Business continuity plans benefit from a regular BCP Auditing exercise program. All incidents, disruptions and emergencies provide lessons learned that could result in a thorough review and update of the plans.

Readiness: BCP testing and feedback on the gaps to the analysis phase for performing an iterative test will provide readiness to the BCP process. BCP Auditing will facilitate to capture lessons learned from the real events and exercises. It should be made available to the business continuity staff so as to provide useful material to make suitable changes and improvements to the business continuity plans as required.

BCP Auditing control objective is to also ensure that the training and instructions have been developed to support the BCP program. Specialised training is required for the Business Continuity specialists and planners.

VIII. CONCLUSION

BC/IT Continuity Plan should be viewed as a methodology, which should be reviewed periodically to keep it abreast of the changes in the technology, organisation, locations, people, applications, and for that matter all that constitutes it. One of the best practices is to keep using the Disaster Recovery Centre (DRC) equipment during the normal operations. IT people can configure the running workload in 80:20 or 90:10 ratios between the main and the DR systems. This ensures the availability of the DR Systems at the time of a disaster. Imagine, if it's not done and the company is hit by a real disaster. When IT staff switches the users to the DR System and if the DR system is not working, it will be a double whammy. BCP/IT Continuity is an ever evolving process in any organisation.

REFERENCES

[1] Saud Bahwan Group's *Business Continuity Plan.*
[2] IBM Power System updates.
[3] IBM Redbook.

Pradeep K Juneja, FIETE. An alumnus of Delhi Technology University (Erstwhile Delhi College of Engineering) and Indian Institute of Technology Delhi. Has more than 45 years of experience in the IT Industry. Specializes in IT strategies, technical management, computer networking, marketing, planning, consultancy, vendor management, key accounts management, contracts management, e-commerce, training, data communication, digital packet radio, environmental engineering and data centre operations. Well conversant with networking, ITU, ISO, IEEE Standards etc.

He worked in Britannia, Continental Devices India Limited, CMC Limited (Now part of TCS) and Saud Bahwan Group, Muscat, Oman. Was Project Coordinator for the planning, design and implementation of India's first National Computer Network- INDONET. Invented a formula for divisibility of prime numbers. Project In-charge for India's first commercial digital packet radio Equipment as part of INDONET. Authored many technical papers.

Presently provides consultancy in the areas of IT Automation, infrastructure and process optimisation. Guest speaker at IIT, Delhi, Delhi Technology University, IETE etc.