Business Continuity Management for Information Technology

What is BCM ?

A subject that covers disaster recovery, crises management, risk management controls and Technology recovery. An issue, which explore the approach of Business Continuity in case of a Disaster, with minimum resources, and maximum output.

The obvious visionary problem of issue that it is considered as a subject, which applies on Private sector, or a subject, which is an Information Technology concern. Practically BCM applies on all Business whether Private or Public and every department either IT or Production. According to Business Continuity Institute Good Practice Guidelines BCM applies equally on Management & Operational staff as well as Technology and geographical location.
To initiate with, I pen down the Business continuity aspect for Information Technology, and will continue to write about BCM for other business segments in near future.

Why BCM for Information Technology?

Increased dependence on IT:

Businesses with dependency of Information technology are most vulnerable victim of any disaster. Starting from Data entry to month end posting, each operation is dependable on various process including technology and human interference. Hardware using OS, carrying Databases, running applications, entering data, collecting documents are dependable operations, of each other. One layer disturbance can hold the operations with in no time.

More interactivity with outside world:

The Customer Database in a excel file which costs you several years of Business can be easily emailed to any of your competitor

Internet made every computer sharable for other computer connected on the Internet. In a latest research, 10 Major Threat have been explored for Internet users which are as follows;

1 Vulnérable CGI and extension on web server
2 Remote Procedure (NFS and Remote execution)
3 IIS Remote Data Services (for example .htr files)
4 Sendmail Buffer Overflow
5 Solaris sadmind and mountd
6 IMAP/POP buffer overflow or incorrect configuration
7 Default SNMP community strings set to 'public' and 'private.'
8 Global file sharing (netbios, Macintosh web sharing, UNIX NFS)
9 Use of weak password or no password on user id
10 Bind Weaknesses

Broader Availability:

Technological advancement like Local Area Networks, Wide Area Networks and wireless network, made data widely available to users. With small mismanagement, the same data will be accessible to unwanted users hence can create immediate problems to your Business Continuity. The Tender Document, which you have planned to submit next morning, with little efforts, can ruin your business targets of the Year.

Making the desired data at desired time is most important part of Business Operations. Securing Network traffic, files and stopping External intrusion are the part of BCM. Cold sites, Warm site and hot sites are the major modalities apply on data broader availability for Business continuity in case of any disaster.

Explosion of Data:

In fact, data is easier to create than to Manage, secure and administrate. Just of small network of users, carry several formats and types of data traveling spontaneously. Application's data (Entered by an application on any Database like Oracle, SQL DB), Documented Data (Quotations, Proposals, Inquiries, Contacts) Emails (PST files) and various independent applications are depending source of any IT Operation. All Businesses depending on any sort of Computers in Operation are equally important to the business. Managing these data is a thorough activity, and making this data available in case of any disaster is serious responsibility.

Risks Abound

While applying BCM on IT segments, following are the risks, to be addressed comprehensively.

- **Viruses and worms**
- **Human error**
- **Employee sabotage**
- **Hackers**
- **Power outages and infrastructure issues**
- **Natural disasters**
- **Terrorist and other attacks**
- **Hardware and software failure**

Figures don't lie:

43 percent of companies that experience a disaster but have no BCP in place ever reopen. 90 percent of them are out of business in two years.

(University of Texas study)

80 percent of companies indicated they had been the subjects of a hostile attack in the form of hacking, viruses or Denial of Service attacks.

(IDC survey)

From Where to Start?

1) Know your Business

Having identified the mission critical processes and functions it is important to determine what the impact would be upon the organization's goals if these were disrupted or lost. Once having identified those critical processes and functions, a risk assessment can be conducted to identify the many threats to these processes. Whatever risks the organization faces, there are relatively few effects, for example: loss of critical system(s), site or personnel or denial of access to systems and premises, all of which produce similar disruption. To this end, the Business Impact Analysis enables the organization to focus risk assessments on essential business elements rather than conduct a global risk-specific analysis. The process will also take into account the time sensitivity of each business function / process to disruption and this information will determine the recovery objectives.

2) Define the threats

As an old saying says, "knowing your enemy is more important than to know your friends". In the same context, its important to define each Threat explored to you business continuity. At the end of this activity, you will notice that many possibilities exist like,

- **Do nothing –** in some instances the board may consider the risk commercially acceptable

- **Changing or ending the process –** deciding to alter existing procedures must be done bearing in mind the organization's key focus
- **Insurance –** provides financial recompense / support in the event of loss, but does not provide protection for brand and reputation
- **Loss Mitigation –** tangible procedures to eliminate / reduce risk
- **Business Continuity Planning –** an approach that seeks to improve organizational resilience to interruption, allowing for the recovery of key Business and systems processes within the recovery time frame objective, whilst maintaining the organization's critical functions.

3) Documentation of Plan

The core document, carrying all these information and Planning, will be Business Continuity Plan (BCP-Manual). This document brings together the actions to be taken at the time of an incident, who is involved and how they

are to be contacted. The plan or plans must reflect the current position of the organization and all it stakeholders. A BCP should be designed to provide recovery of the organization within the recovery time objectives established during the BIA process.
In developing of the plan consideration must be given to:

- **The use of planning aids, plan development and maintenance tools**
- **Inclusion of job descriptions for those involved in delivering the plan**
- **What action plans and checklists should be provided**
- **What information databases and other supporting documentation are required**
- **The recovery team description, responsibilities and organization**
- **Support staff required including recovery and group co-coordinators**
- **The location and equipping of the Emergency (Crisis) Operations Center**

Conclusion

Sufficient Research is available for Business Continuity Managements and Planning, on several Portals, Associations and

Group on Internet. BCP is more a continues process than a generic Plan, so regular research and amendments in the plan is the most appropriate factor to make your plan practically applicable, in case of any disaster. Specialized Consulting is also available for this segments from various companies with in the region.

Experts say that the "Best thing for any BCP is that Disaster should not occur" but this is not the statement to be relaxed.

Links for more resources

http://www.dri.org
http://www.acp-international.com/partners.html
http://www.continuitycentral.com/contact.htm
http://www.plan-it-control-it.com/
http://www.globalcontinuity.com/

Views, comments and critics are always appreciated at

gawasti@yahoo.com
Me-bcp@yahoogroups.com

Writer's Profile

I am a Graduated in IT, served in various Organization of Saudi Arabia, having intense observation on the regional growth in IT Sector specially IS Security, from last six years. Recently engaged with E-Security Gulf Group WLL. to execute the Business Operation In Saudi Arabia. I can be contacted for any details or clarifications on this subject gawasti@yahoo.com or Cell +966-059660016. More details can also be downloaded from

http://finance.groups.yahoo.com/group/me-bcp/