Business Continuity and Disaster Recovery Experience in E-Business in Indian Banks

Shirshendu Maitra
Asst. Professor, Thakur Institute of Management Studies
Career Development & Research
Mumbai, Maharashtra, India

Dr. Meera Shanker
Associate Professor and Head (Management), JDBIMS
SNDT Women's University
Mumbai, Maharashtra, India

Pankaj K. Mudholkar
Asst. Professor, Thakur Institute of Management Studies
Career Development & Research,
Mumbai, Maharashtra, India

Abstract- Business entities today exist in a highly competitive world. Internet banking has now become a global phenomenon. Almost every banking institution all over the world has embraced this technological system of banking due to the numerous benefits it brings, both to the banks themselves and their clients or customers notable among them are convenience and time-saving in doing transactions.

The Internet is now being considered as a strategic weapon and will revolutionize the way banks operate, deliver, and compete against one another, especially when competitive advantages of traditional branch networks are eroding rapidly.

And yet, the threats of disaster, on account of business interruption, are not extinct – in fact, they have also evolved along with the technology. Business interruption does happen – but what is of significance is, how much of the consequences of such interruptions can the business afford. Business Continuity Planning is the act of

proactively working out a way to prevent, if possible, and manage the consequences of a disaster, limiting it to the extent that a business can afford.

This paper presents the preliminary findings of a research study to identify the essential ingredients of successful BCM implementation based on experiences of banks in India. The paper outlines the business continuity planning as a methodology that could be used by organizations in order to reduce the risks that occur both at the organizational level and in its outside environment. There are presented the main objectives and steps in business continuity planning process. In the end of the paper are presented some issues that organizations should take into consideration in the implementation of business continuity planning process projects.

Keywords – E-Business, .BCP, risk assessment, risk management,

I. INTRODUCTION

The term "e-Business" has a very broad application and means different things to different people. Furthermore, its relation with e-commerce is at the source of many disagreements. (Melão, 2008) Some authors view e-Business as the evolution of e- commerce from the buying and selling over the Internet, and argue that the former is a subset of the latter.

Continuing technological innovation and competition among existing banking organizations and new market entrants has allowed for a much wider array of electronic banking products and services for retail and wholesale banking customers. These include traditional activities such as accessing financial information, obtaining loans and opening deposit accounts, as well as relatively new products and services such as electronic bill payment services, personalized financial "portals," account aggregation and business-to-business market places and exchanges.

But any type of e-business interruptions can occur anywhere, anytime. Massive hurricanes, tsunamis, power outages, terrorist bombings and more have made recent headlines. It is impossible to predict what may strike when. In today's 24x7x365 world, it has become mandatory to prepare for such disaster scenarios. Under this circumstance and with the ever increasing dependence on banks for both electronic and traditional banking services, it has become almost mandatory for the banking industry to plan for 'Business Continuity'(BCP).

Most organizations, including banks, nowadays depend on the information technology (IT) on their key business functions. In fact, IT is considered "a vital component for conducting business" (Jacques & Rossouw, 2004). Using simple logic, the value of the IT services for an organization can be known by understanding the impact on the business in case of failure in IT systems. Consequently, upon this understanding, organization management undertakes the right actions to ensure the continuity of information technology services (John R. Harrald, 1999).

II. DR AND BCP

With the ever increasing dependence on banks for both electronic and traditional banking services, it has become almost mandatory for the banking industry to plan for 'Business Continuity.

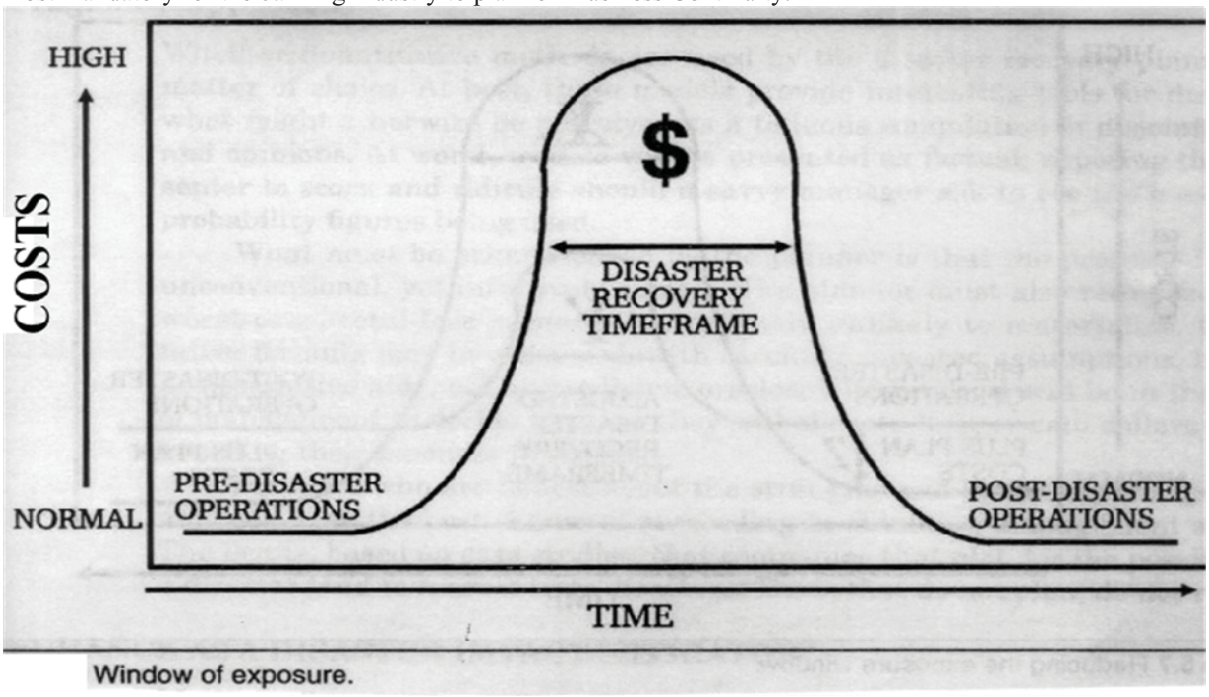

Fig 1: Costs of DRP/BCP

It may sound cliché to mention that much of the commercial activity that we see today is dependent on banks. Banks, in turn, have turned to increasingly complex technology and business models to deliver the services expected in this age of boundary less commerce.

Sophisticated and interconnected Automated Teller Machine (ATM) networks, Tele-banking, Core Banking Solutions and Internet Banking Solutions for seamless customer access are but some of technologies currently deployed. Add to this, the ever expanding branch network to provide banking services in semi-urban and rural areas in India. With this background in mind, it is indeed worrying to imagine a scenario where a disaster may render a bank inoperative for an extended period of time. From Fig 1. It is imperative that the costs of operation only increases by not having a proper BCP/DRP in place. The floods in Mumbai brought to fore one such concern for banks. Bank ATM terminals are

typically located on the ground floor of premises with the backup power generator being located in the basement. The unprecedented floods of July 2005 made all such ATMs non-functional. In such crisis situations, lack of access to financial resources could have severe repercussions. Without these resources, organizations and individuals would find it daunting to take measures to recover from the disaster. This would compound the already difficult situation being faced and could lead to anarchy and situations like run on banks.

Business continuity (BC) in IT has been of interest to many IT professionals. It is a very big subject and many studies have been conducted to address different aspects of it (Wing S. Chow, 2000). Some researches focused on the high level planning and management side of it which led to introducing processes inside the organizations such as business continuity management (BCM) and business continuity planning (BCP) processes. Others focused on the technical part of it which led to introducing technical business continuity solutions such as fault-tolerant systems and data replication solutions.

Business Continuity Planning (BCP) lifecycle is an iterative continuous process that involves business risk and impact analysis, preparation of required emergency procedures, testing and auditing recovery procedures, staff training and awareness of recovery procedures, and maintenance of the business continuity plan (Mick Savage, 2002). The purpose of the BCP is to keep organization business running. This is achieved by creating a plan that addresses how the recovery of key business functions will be in case of incident or a disaster.

III. Risk Assessment

Risk assessment is the exercise of identifying and analyzing the potential vulnerabilities and threats. The sources of risks could be:

- community-wide hazardous events
- accidents or sabotage causing extreme material disaster
- security threats, network and communication failures
- disastrous application errors

Each of these areas should be looked at in the light of the business and the exact possible source located. For each source identified:

the magnitude of the risk and

the probability of its occurrence

must be evaluated to judge the extent of risk exposure. Risk exposure is the easiest way to know how much attention needs to be paid to a source of risk.

Planning is done for both — prevention and control. Accidents and sabotage can be prevented using measures of physical security and personnel practices. Vulnerability assessment and reviews of existing security measures can throw up areas where access control, software and data security, or backups are required. Application errors can be prevented by effective reviews and testing during the software releases.

If needed, the expertise of external agencies can easily be called upon to analyze, devise and put in place some of the preventive measures. The tougher part is to come up with activities for controlling the effects of disaster, and this necessitates a detailed business impact analysis. The end result of the Risk Assessment should be a risk-benefit analysis statement giving the exact threats, and the estimated exposure together with the contingency and mitigation actions required, and also the benefits arising out of covering the risk. This statement should also delineate any assumptions or constraints that exist. Often, this exercise will show that the complete physical disaster has a remote probability of occurring and application crashes, or security break-ins are very frequent.

However, only having a procedure for handling catastrophic disasters without a plan for application failure or vice versa is not advisable. The solution is to prepare a BCP for the worst-case, i.e., complete destruction of the site providing the services. Any other outage can then be easily tackled using a sub-set of the main plan.

IV. Components of a Typical Successful E-Commerce Transaction Loop

Common barriers include: unsuitability for the type of business; enabling factors (availability of ICT skills, qualified personnel, network infrastructure); cost factors (ICT equipment and networks, software and re-organization); security and trust factors (security and reliability of e-commerce systems, uncertainty of payment methods, legal frameworks and Intellectual Property Right); and challenges in areas of management skills, technological capabilities, productivity and competitiveness (OECD, 2004). Lack of reliable trust and redress systems and cross-country legal and regulatory differences also impede e-business adoption (OECD, 2004).

It is however important to note that barriers to e-Business adoption work differently according to organizational type and culture. Areas of training and people development need to be addressed. (Aranda-Mena and Stewart, 2005).

E-commerce does not refer merely to a firm putting up a Web site for the purpose of selling goods to buyers over the Internet. For e-commerce to be a competitive alternative to traditional commercial transactions and for a firm to maximize the benefits of e-commerce, a number of technical as well as enabling issues have to be considered.

A typical e-commerce transaction loop involves the following major players and corresponding requisites:

The Seller should have the following components:

- A corporate Web site with e-commerce capabilities (e.g., a secure transaction server);

- A corporate intranet so that orders are processed in an efficient manner; and
- IT-literate employees to manage the information flows and maintain the e-commerce system.

Transaction partners include:

- Banking institutions that offer transaction clearing services (e.g., processing credit card payments and electronic fund transfers);
- National and international freight companies to enable the movement of physical goods within, around and out of the country. For business-to-consumer transactions, the system must offer a means for cost-efficient transport of small packages (such that purchasing books over the Internet, for example, is not prohibitively more expensive than buying from a local store); and
- Authentication authority that serves as a trusted third party to ensure the integrity and security of transactions.

Consumers (in a business-to-consumer transaction) who:

- Form a critical mass of the population with access to the Internet and disposable income enabling widespread use of credit cards; and
- Possess a mindset for purchasing goods over the Internet rather than by physically inspecting items.

Firms/Businesses (in a business-to-business transaction) that together form a critical mass of companies (especially within supply chains) with Internet access and the capability to place and take orders over the Internet. Government, to establish:

- A legal framework governing e-commerce transactions (including electronic documents, signatures, and the like); and
- Legal institutions that would enforce the legal framework (i.e., laws and regulations) and protect consumers and businesses from fraud, among others. And finally, the Internet, the successful use of which depends on the following:
- A robust and reliable Internet infrastructure; and
- A pricing structure that doesn't penalize consumers for spending time on and buying goods over the Internet (e.g., a flat monthly charge for both ISP access and local phone calls).

For e-commerce to grow, the above requisites and factors have to be in place. The least developed factor is an impediment to the increased uptake of e-commerce as a whole. For instance, a country with an excellent Internet infrastructure will not have high e-commerce figures if banks do not offer support and fulfillment services to e-commerce transactions. In countries that have significant e-commerce figures,a positive feedback loop reinforces each of these factors.

V. RESULTS

The results of the analysis were organized so that a series of benchmarks could be established (see Table 1). As mentioned in previous sections, these benchmarks relate to IT disaster recovery planning activities, not parts of actual plans. They are grouped according to the seven categories of activities, and are summarized on the following table. The third column on the table indicates the percent of banks which perform each process.

Category	Elements	% Performing Activity
Analyzing IT services	IT Services Identification	68.9%
	Prioritizing IT Services	71.1%
	Risks to IT Services	73.2%
Preparing organizational members	Decision Making	75.2%
	Personnel Briefing	65.7%

	Response Team Training	69.9%
Devising means of IT disaster identification and notification	Means of Warning / Communication	75.6%
	Detection	69.8%
	Warning	66.4%
Developing procedures for restarting systems	Recovery Procedures	90.4%
	Alternative Facilities	81.1%
Creating a schedule for backup procedures		93.7%
Selecting offsite storage facilities	Portability	83.8%
	Offsite Backup Locations	79.4%
Creating maintenance schedules	Testing and Updating	89.5%
	Synchronizing	88.7%
	Documentation	87.3%

Table 1 : Results of study

Nearly all banks included in the study meet the IT disaster recovery planning guidelines specified by regulatory bodies. In general, these requirements may be considered the core-technical elements of IT disaster recovery. They include activities such as: creating backup copies of data and software, acquiring alternative technologies, and developing ways of resuming services.

VI. SUMMARY

As per the survey the following factors critical to implement reliable BCM structure and practices .Establish and nurture partnerships with agencies that work in a collaborative mode in supporting banking operations with technology.

a) The customers and partners hold an esteem value about the bank and that is not only a catalyst for progress, but also provides strong support during the phase when the bank is attempting to recover from a disaster.

b) A wider customer base served with a variety of products and supported on multiple delivery channels ensures higher degree of continuity, both in terms of operations and preparedness of a bank in dealing with disruptions in services.

c) Most banks consider state-of-the-art technology as critical to growth and efficient delivery of service. Some large banks also do not want to give up manual processing which they consider as the last resort in effecting transactions during a major discontinuity.

With regard to the current status of BCM practice, the following are important:

a) Banks have put together reliable IT Infrastructures to support their operations. These are built using high-end platforms and proprietary solutions. Certain banks also have custom-built solutions developed by in-house teams using open-source software to attain vendor independence.

d) All banks that have achieved high degree of computerization have modern central data centers with distant DR Sites. The DR site utilization percentage was, however, found to vary significantly. Only a few banks are more regular with putting the actual load on DR Sites frequently.

e) The composition of teams managing IT in banks is mostly a judicious mix of Banking and Systems professionals to foster a rich blend of knowledge of banking processes and technology.

f) The advanced practices of server and storage consolidations to optimize data storage and processing have been implemented in the banks studied.

g) Security at both database and systems levels has been implemented in most banks using complex and comprehensive third-party solutions.

h) The Network and Systems Administration are carried out using remote control solutions ensuring greater reliability and efficiency.

Most banks have built sufficient redundancy in their information and communication technology components to ensure a high degree of reliability.

VII..CONCLUSION

Business Continuity Planning is not just relevant for business organizations that offer e-business services using IT and that handle a lot of data. It is also significant for IT service providers. Their development centres and support units have a wealth of knowledge and all their past experiences are in the form of sources and documents on the servers and tape libraries. They have a dual responsibility — to plan for their own continuity, as well as that of their customers. Planning for continuity is about being safe — safe from the consequences of events that one hopes will never happen; and the truth is — it is always better to be safe than sorry.

REFERENCES

[1] 1. Aranda- Mena, G and Stewart, P (2005) " Barriers to e-business adoption in construction international literature review" July 2005 2nd edition.

[2] 2. Aidan Berry and E. Jarvis (1993). "Accounting for decision making: resource constraints and decisions which are mutually exclusive". Accounting in a Business Context . Chapman & Hall: pp:401.

[3] 5. Carol V. Brown, Daniel W. DeHayes, Jeffery A. Hoffer, E. Wainright Martin, William C. Perkins. "Managing IT in an E-world". Managing Information Technology . Person Prentice Hall: pp 1.

[4] 6. Charles O. Omekwu (2006). "African clustuer and libraries: the information technology challenge". The Electronic Library. Vol 24. No 2. pp 243-264.

[5] 7. Charles Cresson Wood (2002), Information Security Policies Made Easy, Information Shield Inc.,pp: 202-210

[6] 9. Gary Donlon (2004). "IT Service Continuity: Know the unknowns". Service talk. Issue No 66. pp:38-39.

[7] 10. Geary W. Sikich(2003), Business Continuity: Maintaining Resilience in Uncertain Times, Pennwell Books,pp:234-240

[8] 11.H. Frank Cervone (2006). "Managing digital libraries: the view from 30,000 feet. Disaster recovery and continuity planning for digital library systems". OCLC Systems & Services. Vol. 22 No. 3. 173-178.

[9] 12. Jacques Botha & Rossouw Von Solms (2004). "A cyclic approach to business continuity planning". Information Management & Computer Security. Vol 12 ,pp:328-337.

[10] 13. James C. Barnes (2003), A guide to Business Continuity Planning, John Willey & Sons, ISBN:13-978-0-8144-1613-6,pp 125-132

[11] 14. John William Toigo(2002), "Disaster Recovery Planning:Preparing for the Unthinkable", 3rd Edition, Prentice Hall,pp:19-54

[12] 15. Joshua Weinberger (2004). "Averting Customer Data Loss". Customer Relationship Management. Vol 3, p 16.

[13] 16. Kakoli Bandyopadhyay & Peter P. Mykytyn & Kathleen Mykytyn (1999). "A frame work for integrated risk management in information technology". Management Decision. Vol 37 No 5. pp: 437-444.

[14] 17. Leon Erlanger (2006). "In case of emergency activate business continuity plan". InfoWorld. pp:27-31.

[15] 18. Dr. Manik Dey(2011),Business Continuity Planning (BCP) methodology –Essential for every business,ISBN:978-1612-84-119-9

[16] 19.Maria Cirino(2007), The Art of Comprehensive Vulnerability Management (Black Book Series), Larstan Publishing,pp: 156-162

[17] 20. Melão, N. (2008)" E-Business, E-Business PROCESSES AND E-Business Melão, N. and Pidd, M. (2000) "A Conceptual Framework for Understanding and eBusiness Progression", Journal of Computing and Information Technology, vol. 13, No. 2, pp. 123-136.

[18] 21. Mick Savage (2002). "Business continuity planning". Work Study. Vol 51 No 5. pp:254-261

[19] 22. Montri Wiboonrat, Kitti Kosavisutte(2008), Optimization Strategy for Disaster Recovery :ISBN 978-1-4244-2330-9

[20] 23. Nijaz Bajgoric(2006). “Information technologies for business continuity: an implementation framework”. Information Management & Computer Security. Vol 14 No.5. pp:450-466

[21] 24. Peter H. Gregory CISA CISSP, Philip Jan Rothstein (2007), IT Disaster Recovery Planning For Dummies: ISBN: 978-0-470-03973-1

[22] 25. Rentsch, T(1982), Object Oriented Programming”; SIGPLAN Notices; Vol.17 ; pp:51

[23]

[24] 26. Rick A. Myer, Christian Conte & Sarah E. Peterson (2007). "Human impact issues for crisis management in organizations". Disaster Prevention and Management. Vol 16. pp:761-770

[25] 27. Rudolph C.G(1990), “Business Continuation Planning/ Disaster Recovery: A Marking Perspective.” HBS, Pp 25-28.

[26] 28. Russell Smith (1995). "Business continuity planning and service level agreements". Information Management & Computer Security. Vol 3 . pp:17-19

[27] 29. Samuel Certo and Trevis Certo (2006). “ Making Decisions”. Modern Management (10th ed). Prentice Hal: pp:161

[28] 30. Samuel Certo and Trevis Certo (2006). “Strategic Planning”. Modern Management (10th ed). Prentice Hal: p:180

[29] 31. Scott, D. (2002), Best Practices and Trends in Business Continuity Planning, Gartner Symposium ITxpo 2002, Gartner, Inc.,pp: 230-235

[30] 32. Sharman Lichtenstein (1996). "Factors in the selection of risk assessment method". Information Management & Computer Security. Vol 4 No. 4. 20-25

[31] 33. Sharon Halliday, Karin Badenhorst & Rossouw Von Solms (1996). "A business approach to effective information technology risk analysis and management". Management & Computer Security. Vol 4 ,pp: 19-31

[32] 34. Stewart H.C. Wan & Yuk-Hee Chan (2008). “ Improving service management in campus IT operations”. Campus-Wide Information Systems. Vol.25 No. 1. pp:30-49

[33] 35. Stewart Wan (2009). "Service impact analysis using business continuity planning process." Campus-Wide Information Systems. Vol 26. No. 1. pp:20-42

[34] 36. Susan Snedaker(2007), Business Continuity & Disaster Recovery for IT Professionals. Publisher: Syngress. ISBN-10: 1-59749-172-34, pp:34-40

[35] 37. ThuyUyen H. Nguyen (2008). “Information technology adoption in SMEs: an integrated framework”. International Journal of Entrepreneurial Behavior & Research. Vol 15 pp:162-186

[36] 38. Tillal Eldabi, Zahir Irani, Ray Paul & Peter E. Love (2002). “Quantitiative and qualitative decision-making methods in simulation modeling”. Management Decision. Vol 40 pp:64-73

[37] 39. Wing S. Chow (2000). "Success factors for IS disaster recovery planning in Hong Kong". Information Management & Computer Security. Vol 8 No. 2. pp:80-86.

[38] 40. Young-Fai Lee & John R. Harrald (1999). "Critical issue for business area impact analysis in business crisis management analytical capacity". Disaster Prevention and Management. Vol 8 No 3. pp:184-189