Protecting E-Business by implementing Business Continuity and Disaster Recovery Planning in the Banking Industry

Pankaj K. Mudholkar
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

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

Abstract- Banks today are becoming increasingly aware of both the threat and the opportunity that the web represents. Banks are providing ICT – mediated e-business services such as automated teller machines, electronic fund transfer, electronic smart cards, credit cards, and debit cards, mobile banking, which are transforming the traditional ways of banking and providing competitive edge for banks that provide those services. But, to be competitive in the Internet economy, companies need to harness the power of the Internet successfully; hence it is important to understand risk and responses in the adoption of e-business.

The significance of this study can be seen in the fact that the outcome can be applied in providing e-business services in more secured way by knowing the risk factors involved in e-business. This paper discusses how business continuity and disaster recovery plans should be implemented to overcome risks of using e-business services in the banking sector. The study objectives are to describe risks which come from factors including online fraud and disruptions to their information technology systems. It deals mainly with the business continuity and disaster recovery planning in the banking industry.

Keywords – E-Business, .BCP, Risk, Information System, Internet, Security.

I. Introduction

E-Business (Electronic business) is the use of Internet-based information and communication technologies (ICTs) to conduct business (including sharing information, maintaining relationships and conducting transactions) within and between organizations (Poon and Swatman, 1997) [26].

Banking organizations have been delivering e-business services to consumers and businesses remotely for years. These services offer numerous benefits to the banks and the customers. We can check account balances, transfer money, pay bills, collect receivables and ultimately reduce transaction costs and establish great control over bank accounts.

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.

Notwithstanding the significant benefits of technological innovation, the rapid development of e-banking capabilities carries risks as well as benefits and it is important that these risks are recognized and managed by banking institutions in a prudent manner.

As E-Business is mainly built upon the concept of doing businesses online, it includes, information sharing, multi-party collaboration, design for supply chain management, postponement for mass customization, outsourcing and partnerships, and extended or joint performance measures. It allows the E-Business organizations to come up with highly innovative solutions that accelerated the widespread adoption of various activities. But even a detailed and thoughtful approach to the Web does not guarantee business success. The main purpose behind the launching of online banking services is to provide the customers with an alternative, more responsive and with less expensive options. With options just a click away, customers have more control than ever. They expect real-time answers and superior usability. They also want personal attention and highly customized products and services. The focus of e-business must always be on the customer. On the other hand, the technology and the business structure follow on form of the value you intend to provide to the customer.

Despite the benefits of e-business services to the banking sector, there has been little research done on the e-business risk and responses in the banking industry in India.

II. E-Business and Banks

The introduction of E-Business has had a significant impact on banks operating with physical branches. Especially the internet has made it possible for banks to cut cost by offering online banking at a lower cost. The econometric analysis show that ICT use is positively correlated with firm restructuring activities. Thus, ICT enables companies to redefine the boundaries of their organizations and possibly gain a competitive advantage.

The various areas where the banks are preparing to use e-business approach include familiar and relatively mature electronically based products in developing markets, such as telephone banking, mobile banking, credit cards, ATMs, and direct deposit. This means that most of the banks have recognized the need to change their business process to conform to changing business trends in order to keep up with competition.

E-Business services provide customer access to accounts, the ability to move their money between different accounts, and making payments or applying for loans via e-Channels.

A large number of organizations from within and outside the financial sector are currently offering an e-business service which includes delivering services using Wireless Application Protocol (WAP).

Many people see the development of E-Business services in the banking sector as a revolutionary development, but, broadly speaking, these services could be seen as another step in banking evolution. Just like ATMs, it gives consumers another medium for conducting their banking. The fears that this channel will completely replace existing channels may not be realistic, and experience so far shows that the future is a mixture of "clicks (e-banking) and mortar (branches)". Although start up costs for an internet banking channel can be high, it can quickly become profitable once a critical mass is achieved. The customers are using net banking, to pay the utility bills, insurance premium, to book orders online, to book railway tickets also to book flight tickets, purchasing the products online using net banking or online banking (e-banking), credit cards, debit cards or smartcards also.

III. E-Business: BCP And Disaster Pecovery Planning In Banks

A Business Continuity Planning (BCP) specifies how your E-Business will resume partial or complete operations after a major disruption or risks, such as strategic risks, business risks, transactions or operations risks, credit risks, liquidity, interest rate and price-market risk, reputational risks, a natural disaster, or a terrorist attack. Business Continuity Planning includes :

- Identifying events that might lead to a business interruption
- Assessing how disruptive events might affect your e-business
- Determining the resources you will need to maintain critical business functions after disruptive events
- Developing a disaster recovery plan for critical business systems

The term “disaster recovery planning” is sometimes used interchangeably with business continuity planning; disaster recovery planning is generally associated with the technological aspects of a business continuity plan. Disaster recovery planning deals with the specific resources and procedures needed to recover from hardware failures, loss of power, loss of communication lines, or other unexpected and catastrophic events that interrupt the operation of business system.

Financial institutions must be prepared to protect e-business’s future by managing both the general risks inherent in operating any business and the specific risks associated with operating an e-business. Securing e-business to protect not only physical assets but also its reputation and longevity is a serious issue.

The risks associated with the e-business are categorized as-

3.1 Strategic Risk –

A financial institution’s board and management should understand the risks associated with e-business services and evaluate the resulting risk management costs against the potential return on investment prior to offering e-business services. Poor e-business planning and investment decisions can increase a financial institution’s strategic risk. On strategic risk E-Business is relatively new and, as a result, there can be a lack of understanding among senior management about its potential and implications. People with technological, but not banking skills can end up the driving initiatives. E-initiatives can spring up in an incoherent and piecemeal manner in firms. They can be expensive and can fail to recoup their cost. Furthermore, they are often positioned as loss leaders (to capture market share), but may not attract the types of customers that banks want or expect and may have unexpected implication on existing business lines.

Banks should respond to these risks by having a clear strategy driven from the top and should ensure that this strategy takes account of the effect of e-business, wherever relevant. Such a strategy should be clearly disseminated across the business, and supported by a clear business plan with an effective means of monitoring performance against it.

3.2 Business Risk –

Business risks are also significant. Given the newness of e-business services such as e-banking, nobody knows much about whether e-banking customers will have different characteristics from the traditional banking customers. They may well have different characteristics. This could render existing score card models inappropriate, this resulting in either higher rejection rates or inappropriate pricing to cover the risk. Banks may not be able to assess credit quality at a distance as effectively as they do in face to face circumstances. It could be more difficult to assess the nature and quality of collateral offered at a distance, especially if it is located in an area the bank is unfamiliar with (particularly if the is overseas). Furthermore as it is difficult to predict customer volumes and the stickiness of E-deposits (things which could lead either to rapid flows in or out of the bank) it could be very difficult to manage liquidity.

Of course, these are old risks with which banks and supervisors have considerable experience but they need to be watchful of old risks in new guises. In particular risk models and eve processes designed for traditional banking may not be appropriate.

3.3 Transaction/ Operations Risk –

Transaction/ Operations risk arises from fraud, processing errors, system disruptions, or other unanticipated events resulting in the institutions inability to deliver products or services. This risk exists in each product and service offered. The level of transaction risk is affected by the structure of the institution's processing environment, including the types of services offered and the complexity of the processes and supporting technology.

In most instances, e-business activities in banking will increase the complexity of the institution's activities and the quantity of its transaction/ operations risk, especially if the institution is offering innovative services that have not been standardized. Since customers expect e-business services to be available 24 hours a day, 7 days a week, financial institutions should ensure their e-business infrastructures contain sufficient capacity and redundancy to ensure reliable service availability. Even institutions that do not consider e-business services in the banking sector a critical financial service due to the availability of alternate processing channels, should carefully consider customer expectations and the potential impact of service disruptions on customer satisfaction and loyalty.

The key to controlling transaction risk lies in adapting effective policies, procedures, and controls to meet the new risk exposures introduced by e-business services in banking. Basic internal controls including segregation of duties, dual controls, and reconcilements remain important. Information security controls, in particular, become more significant requiring additional processes, tools, expertise, and testing. Institutions should determine the appropriate level of security controls based on their assessment of the sensitivity of the information to the customer and to the institution and on the institution's established risk tolerance level.

3.4 Credit Risk –

Generally, a financial institution's credit risk is not increased by the mere fact that a loan is originated through an e-banking channel. However, management should consider additional precautions when originating and approving loans electronically, including assuring management information systems effectively track the performance of portfolios originated through e-banking channels. The following aspects of on-line loan origination and approval tend to make risk management of the lending process more challenging. If not properly managed, these aspects can significantly increase credit risk.

- verifying the customer's identity for on-line credit applications and executing an enforceable contract;
- monitoring and controlling the growth, pricing, underwriting standards, and ongoing credit quality of loans originated through e-banking channel;
- monitoring and oversight of third-parties doing business as agents or on behalf of the financial institution (for example, an Internet loan origination site or electronic payment processor);
- valuing collateral and perfecting liens over a potentially wider geographic area;
- Collecting loans from individuals over a potentially wider geographic area;
- monitoring any increased volume of, and possible concentration in, out-of-area lending.

3.5 Liquidity, interest rate, price/ market Risk –

Funding and investment related risks could increase with an institution's e-banking initiatives depending on the volatility and pricing of the acquired deposits. The Internet provides institutions with the ability to market their products and services globally. Internet-based advertising programs can effectively match yield-focused investors with potentially high-yielding deposits. But Internet-originated deposits have the potential to attract customers who focus exclusively on rates and may provide a funding source with risk characteristics similar to brokered deposits. An institution can control this potential volatility and expanded geographic reach through its deposit contract and account opening practices, which might involve face-to-face meetings or the exchange of paper correspondence. The institution should modify its policies as necessary to address the following e-banking finding issues:

- potential increase in dependence on brokered funds or rather highly rate-sensitive deposits;
- potential acquisition of funds from markets where the institution is not licensed to engage in banking, particularly if the institution does not establish, disclose, and enforce geographic restrictions;
- potential impact of loan or deposit growth from an expanded Internet market, including the impact of such growth on capital ratios;
- potential increase in volatility of funds should e-banking security problems negatively impact customer confidence or the market's perception of the institution.

3.6 Reputational Risk –

This is considerably heightened for banks using the Internet. For example the Internet allows for the rapid dissemination of information which means that any incident, either good or bad, is common knowledge within a short space of time. The speed of the Internet considerably cuts the optimal response times for both banks and regulators to any incident.

Any problems encountered by one firm in this new environment may affect the business of another, as it may affect confidence in the Internet as a whole. There is therefore a risk that one rogue E-bank could cause significant problems for all banks providing services via the Internet. This is a new type of systematic risk and is causing concern to R-banking providers. Overall, the Internet puts an emphasis on reputational risks. Banks need to be sure that customer' rights and information needs are adequately safeguarded and provided for.

E-Business services in the banking sector may suffer from the variety of potential threats:

- natural or human-made disasters such as fire, flood, hurricane, earthquake, or terrorist attack;
- physical theft of your equipment and data storage media or electronic theft of customers data;
- business interruptions caused by vandalism of your web site or outside attacks on your network;
- litigation and settlement costs associated with the inappropriate use of e-mail and the Internet by bank employees;
- product or service claims against items advertised and sold via your web site;
- lawsuits resulting from infringements of web site related copyrights, trademarks, and patents.

Such threats can result not only in immediate loss of revenue, but they can also compromise future revenue and may result in compensatory payments to others for damages. In short, losses from such risks such as these could threaten the very survival of banking e-business. Therefore the banks must have to keep some mechanism in place for managing the risk of potential losses.

Business continuity planning involves the following five major processes:

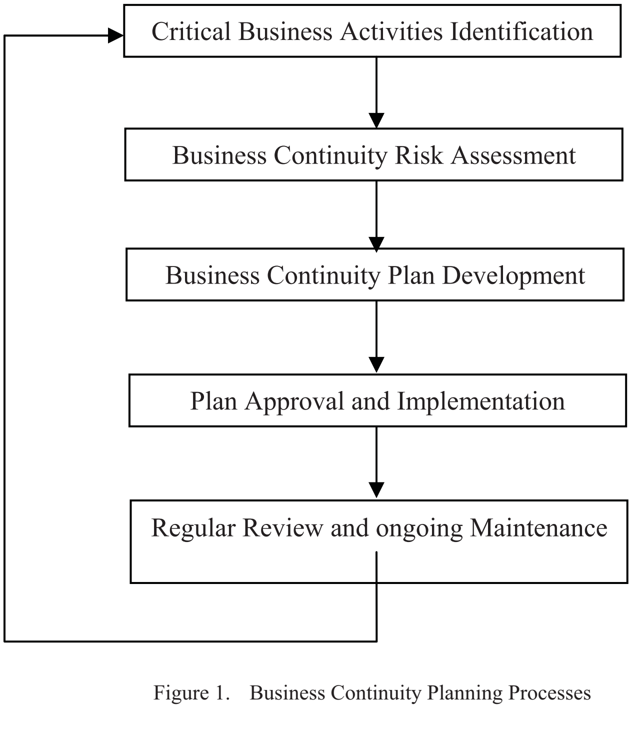
Critical Business Activities Identification
Business Continuity Risk Assessment
Business Continuity Plan Development
Plan Approval and Implementation
Regular Review and ongoing Maintenance

Figure 1. Business Continuity Planning Processes

A business continuity plan should specify a plan of succession for management personnel, identify who is the next in line to assume responsibilities if a manager is not available, and describe procedures for notifying all employees where to report when a disruptive event occurs after work hours.

BCP forms a part of an organisation's overall Business Continuity Management (BCM) plan, which is the “preparedness of an organisation”, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes, at an agreed level and limit the impact of the disaster on people, processes and infrastructure (includes IT); or to minimise the operational, financial, legal, reputational and other material consequences arising from such a disaster.

Effective business continuity management typically incorporates business impact analyses, recovery strategies and business continuity plans, as well as a governance programme covering a testing programme, training and awareness programme, communication and crisis management programme.

This involves the development of a Business Continuity Plan (BCP) designed to ensure the recovery of critical business activities from natural or man-made failures or disasters to an acceptable level within a predefined time frame, thereby minimizing the impact of losses to the organisation. Implementing a BCP is essential for every business.

3.7 *Critical Business Activities Identification –*

It is crucial to understand where a bank needs to focus on in order to recover in case of an incident. The first step in business continuity planning is to identify the most critical business activities to bank’s survival.

Critical business activities are those that must be present to sustain the continuity of business, where failing to performing them would lead to:

- Major revenue losses;
- Failure to meet regulatory or contractual requirements;
- Compromise of operational efficiency, or
- Loss of customer / damage of reputation.

Once the critical activities are identified, perform analysis on each of them to determine the priority and objective on the recovery of critical business activities based on their importance to the bank's achievement of strategic goals. Typical questions to be considered include:

- What are the operational, financial and other competitive impacts to the bank if the activities are not functioned?
- How quickly do the activities need to be back in production for bank to survive?
- How much data and financial losses can bank afford?

For each of the critical business activity identified, it is also necessary to find out all the supporting resources needed to perform the activity and the effect on the business of the unavailability of the resources. Listed below are the areas of resources you should consider:

- People;
- Information technology (service, application, network, data);
- Data and voice communication;
- Paper-based documents and records;
- Physical infrastructure, key equipment and facilities; and
- External services / products dependencies.

3.8 *Business Continuity Risk Assessment –*

A disaster could happen to any company – no matter the business size. Risk assessment on critical business activities should be conducted, identifying possible risks and assessing the likelihood and impact of disruptive events. It is vital that you understand the disruptions that would be disastrous to the running of your business. Different disaster scenarios should be considered, some common threats include:

- Natural disaster, such as earthquake, fire, typhoon, flood;
- Loss of key equipment / information system / facility;
- Disruption of external telecommunications services;
- Utility outage, such as failure of power supply;
- Loss of life, disease, health & safety issues; and
- Terrorism & cyber attack.

Risk assessment against different threats may result in different outcomes. Some may require no action, while some require continuity planning to be developed and supported with additional resources. This will help a company to explore the possible effects of disaster incidents. After that, risks can be prioritized against objectives relevant to the organisation, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities.

3.9 *Business Continuity Plan Development –*

Business Continuity Plan (BCP) allows you to prepare for the worst situation that would keep your business from being operational and to minimise service disruption as well as financial loss. The plan only needs to include the business activities that are most critical to keep your company up and running.

Based on the results from the analysis made on critical business activities and possible risks, you can start developing business continuity and recovery strategies. The selection of strategy may depend upon the criticality of business activities, cost, time for recovery and security.

Listed below are the typical items included in a BCP:

- Individual roles and responsibilities;
- Conditions for its activation;
- Processes to be followed;
- Escalation plan;
- Emergency procedure to handle incident;
- Temporary operational procedure;
- Resumption procedure;
- Fallback procedure; and
- Maintenance schedule and process for testing the plan.

For a small company, a BCP may be simply a printed manual stored safely away from main working location, with emergency contact information, location of offsite data backup storage media, copies of insurance contracts, and other critical material necessary for survival of the business.

The purchase of suitable insurance may be considered as part of the overall business continuity process to recoup losses from risks that cannot be completely prevented or controlled. The decision to obtain insurance should be based on the likelihood and degree of loss identified. Please note that insurance should not be treated as a substitute for an effective BCP since it does not deal with the recovery of business.

Before the plan is put into practice, testing should be conducted to ensure it is effective. Testing may include simulations, business process test, technical recovery and resumption testing, recovery processes testing at alternate site, supplier facilities and services testing etc.

3.10 Plan Approval and Implementation –

Once a Business Continuity Plan (BCP) is developed, it is important that endorsement should be sought for approval and support.

Points to note during the implementation of BCP:

- BCP should be documented and disseminated to all staff to follow before, during and after disruptive event occurred.
- Awareness training and education for staff should be conducted to help them understanding the business continuity processes and their individual responsibilities and actions to be taken when the plan is invoked. This is to ensure the processes would be carried out effectively.
- Copies of BCP should be stored at remote location and kept updated with the same level of security protection as at the main site.
- Other material necessary to execute the BCP and for organisational survival should also be stored at the remote location, such as offsite data backup storage media and copies of insurance contracts.
- A company may also need to have pre-arrangement with external parties to ensure timely resumption of operations, such as facilities access and telecommunication systems.

3.11 Regular Review and Ongoing Maintainance –

In order to validate the business continuity arrangements, testing, review and ongoing maintenance should be conducted regularly to ensure they are up-to-date and effective.

- Regular review, testing & verification of documented Business Continuity Plan (BCP) and the technical solutions should be conducted regularly, say annually.
- When any new or major change in business requirements / environment are identified, the existing procedures should be updated as appropriate.
- Procedures should be included within the organisation's change management programme to ensure that business continuity matters are always addressed appropriately.
- BCP and the test results should also be subjected to independent audit and review.

IV. BCP AND DISASTER PECOVERY PLANNING: E-BUSINESS SECURITY GUIDELINES IN BANKS

Business Continuity Plan should provide business-critical information to be maintained offsite as well as onsite andbe accessible to members of crisis management team. Disaster recovery and business contingency plans should be developed which include the definition of what constitutes a disaster, procedures of what should be done to recover from various failures, and how business will resume. The plan should be tested and periodically reevaluated. Backups and test restores should be performed on a frequent and regular basis. The backup and recovery process, including recovery point and time objectives, should be documented and tested on a regular basis. Consider how you will handle service interruptions or a denial of service. This information may include the following items:

1. The merchant is always responsible for security of the Internet-connected PC where customer details are handled. Virus protection and a firewall are the minimum requirement. To be absolutely safe, store sensitive information and customer details on zip-disks, a physically separate PC or with a commercial file storage service. Always keep multiple back-ups of essential information, and ensure they are stored safely off-site.

2. Sensitive information, especially credit card data, should never be stored on the web server. The data collected by the web server should be passed to another physical machine for storage. Ideally, the data collected by an e-business web site should be stored in a location that is not directly accessible to the Internet. Sensitive information should be stored encrypted when possible. Be wary of sensitive data that may be stored in a web server's cache or log files.
3. The retention of sensitive information such as credit card numbers should be avoided where possible. Sensitive information should be stored on the minimal number of machines while still maintaining system reliability. Care must also be taken to protect sensitive system data such as private keys.
4. Sensitive information should be stored for a minimal length of time. The most sensitive portions of the information should be purged once it is no longer needed (e.g. deleting the customer's credit card number once the transaction has been processed while retaining demographic information).
5. Copies of the data stored on the e-business machines must be treated with the same security precautions as the production data. Backup tapes and removable media must be kept in a secure location, and sanitized or destroyed before disposal. Hard copies, such as reports, containing sensitive data should be stored in a secure location, and properly destroyed (e.g. shredded) when no longer required.
6. All transmissions of sensitive information between the web client and the e-business web server should utilize current industry standard encryption (e.g. 128-bit SSL v3 encryption, with a minimum key length of 1024 bits.) Servers should be configured to refuse clients who cannot accept the required level of encryption, although consider providing a link on the site so customers can download the required version of the browser. Usernames and passwords should not be transmitted over the network in clear text. All administrative connections to the web server should also utilize encryption.
7. System administrators must inspect log files (e.g. security, audit, firewall, antivirus) daily for suspicious activity. Investigate repeated login failures, account management events, failed privilege use, policy changes etc. Logs should have defined maximum sizes and retention periods. Administrators should periodically perform self-audits of the e-business systems. Staff should be informed of basic security practices (e.g. locking workstations, strong passwords) and be wary of social engineering attacks. Inquiries regarding customer information should be referred to individuals who have been trained in safeguarding information. Suspicious activity, including suspected intrusions and significant security violations, should be reported to the supervisor, department's designated Customer Information Security Officer, Police, and for cases involving computer security. Host and/ or network-based intrusion detection systems should be considered as a further security measure.
8. Strong user authentication (e.g. username/password, digital certificate) should be used with web-based systems. Unique user identification and passwords should be used and enforced by the application before each transaction. Passwords should not be visible or retrievable online. IP addresses should not be considered reliable authentication for sensitive information. Consider the use of personal digital certificates or tokens for stronger authentication.
9. The transfer and display of credit card numbers or other sensitive information should be kept to a minimum. Credit card numbers should not be retrievable online. Applications should only display a small portion of the credit card number after if is initially entered by the user. Changes and deletions of the stored credit card number should be allowed without revealing the original number.
10. While using net banking keep password change at first login mandatory and account locking after unsuccessful attempts.

V.CONCLUSION

Banking industry is responding to the contemporary security challenges through a formal security function that derives inspiration from leading security standards for overseeing security initiatives in the banks. Along with aligning the security initiatives to these leading security standards, banks need to invest their energies on providing architectural treatment to security, continuously assessing their exposure to threats through exercises such as threat modeling, applying the guidelines and imbibing the practice of 'security in design by implementing business continuity and disaster recovery plans. This will bring a structured approach in their defense strategies and programs for efficiently & effectively mitigating the real threats by ensuring that security is considered right from the design phase of any product or service. The problem of information security in today's networked world is presented together with current common solutions applied to solve it with reference to the banking industry.

REFERENCES

[1] Alawneh A., and Hattab E (2009), "An Empirical Study of Sources affecting E-Business Value Creation in Jordian Banking Services Sector", International Arab Journal of e-Technology, Vol. 1, No. 2, pp. 1-8

[2] Albert H., Judd, Rivers (2006), "Creating a winning E-Business", Wagner Course Technology Thomson Learning, pp. 37-255

[3] Amit Basu and Steve Muylle (2007), "How to Plan E-Business Initiatives in Established Companies", Vol. 49, No. 1, pp. 28-36

[4] Andreas Crede (1999), "Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems Using the Internet", International Journal of Computer-Mediated Communication, Vol. 1, No. 3, pp. 1-25

[5] Aranda-Mena, Wakefield and Lombardo, P. (2006), "A Diffusion Theoretic Approach to Analysing E-Business Up-Take in Small Building Enterprises", International Journal of IT in Construction - Special Issue on E-Commerce, Vol. 11, No. 1, pp. 149-159

[6] Ayo, Charles K. (2008). "A Framework for e-Commerce Implementation: Nigeria a Case Study", International Journal of Internet Banking and Commerce, Vol. 13, No.2, pp. 1-12

[7] Brahm Canzer (2009) "E-Business and Commerce Strategic Thinking and Practice", Houghton Mifflin, pp. 114-312

[8] Chiemeke, S. C., Evwiekpaefe, A. and Chete, F. (2006), "The Adoption of Internet Banking in Nigeria: An Empirical Investigation", Journal of Internet Banking and Commerce, Vol. 11, No.3, pp 33-49

[9] David Whiteley (2001) "E-Commerce Strategy, Technologies and Applications", Tata McGraw Hill, pp. 3-143

[10] Earl, M. (2001), "Evolving the E-Business" , Business Strategy Review, Vol. 11, No. 1, pp. 33-38

[11] Eben Otuteye (2003) "A Systematic Approach to E-Business Security", International Journal of E-Business, Vol. 9, No. 1, pp. 87-103

[12] Hackbarth, G. & Kettinger W. J. (2000), "Building an E-Business Strategy: Information Systems Management", Journal of Information Systems Management, Vol. 17, No. 3, pp. 1-16

[13] Harris L. and Spence J. (2002) "The Ethics of E-Banking", International Journal of Electronic Commerce Research, Vol. 3, No.2, pp. 59-66

[14] Joseph, P. (2009), "E-Commerce An Indian Perspective", PHI, pp. 304-503.

[15] Kalakota, R. and M. Robinson (1999), "E-Business: Roadmap for success", Addison-Wesley, 112-149

[16] Karjaluoto H., Mattila M. (2002). "Electronic Banking in Finland: Consumer Beliefs and Reactions to a New Delivery Channel", Journal of Financial Services Marketing, Vol. 6, No. 4, pp. 346–361

[17] Laudon, K. and Traver, C. (2008), "E-Commerce: Business, Technology, Society", Prentice Hall, 48-67

[18] Masocha, R., Chiliya and Zindiye (2011), "The Impact of Technology on Competitive Marketing by Banks", African Journal of Marketing Management, Vol. 3, No. 3, pp. 68-77

[19] Melao, N. (2008), " E-Business Processes and E-Business Process Modeling: A State-of-the-Art Overview", International Journal of Services Technology and Management, Vol. 11, No. 3, pp. 293-322

[20] Mendo, F. and Fitzgerald, G. (2005), "Theoretical Approaches to Study SMEs E-Business Progression", Journal of Computing and Information Technology, Vol. 13, No. 2, pp. 123-136

[21] Namita Rajput (2011), "Impact of IT on Indian Commercial Banking Industry: DEA Analysis", Global Journal of Enterprise Information System, Vol. 3, No. 1, pp. 17-31

[22] Nauman Zahid, Mujtaba and Riaz (2010), "Consumer Acceptance of Online Banking", European Journal of Economics, Finance and Administrative Sciences, Vol. 3, No. 27, pp. 44-52

[23] Omar A. El Sawy (2001), "Redesigning Enterprise Processes for E-Business", McGraw Hill, pp. 29-40

[24] Pankaj Shukla and Ruby Shukla (2011), "E-Banking: Problems and Prospects", International Journal of Management and Business Studies, Vol. 1, No. 1, pp. 23-25

[25] Peterson Obara Magutu,(2009), "Modeling the Effects of E-Commerce Adoption on Business Process Management: Case Study of Commercial Banks in Kenya", Journal of International Business Information Management Association, Vol. 8, No. 3, pp. 175-190

[26] Poon S. & Swatam (1997), "Small business use of Internet: Findings from Australian case studies", International Marketing Review, Vol. 14, No. 5, pp. 385-402

[27] Poon S. and Swatman P. (1999), "An exploratory study of small business Internet commerce issues", International Journal of Information and Management, Vol. 35, No.1, pp. 9-18

[28] Rafiu, Oyesola Salawu (2007), "The Emergence of Internet Banking in Nigeria: An Appraisal", Information Technology Journal, Vol. 6, No. 4, pp. 490-496

[29] Rahmath Safeena, Hema Date and Abdullah Kammani (2011), “Internet Banking Adoption in an Emerging Economy: Indian Consumer’s Perspective”, International Arab Journal of e-Technology, Vol. 2, No. 1, pp. 56-64

[30] Rajesh Pal (2009), “Indian Banking and Globalization”, Adhyayan Pub., pp. 33-88

[31] Ravikumar Jain B., Krishna Kishore Puranam (2008), “Internet Banking”, ICFAI University Press, pp. 69-88

[32] Reginald Masocha, Norman Chiliya and Stanislous Zindiye (2011), “The Impact of Technology on Competitive Marketing by Banks: A Case Study Approach”, African Journal of Marketing Management, Vol. 3, No. 3, pp. 68-77

[33] Sana Haider Sumra (2011), ”The Impact of E-Banking on the Profitability of Banks: A Study of Pakistani Banks”, Journal of Public Administration and Governance, Vol. 1, No. 1, pp. 31-38

[34] Sanjay Dhingra (2011), “Measuring IT Effectiveness in Banks of India for Sustainable Development”, International Journal of Information Technology, Vol. 3, No. 2, pp. 17-20

[35] Sawant B. (2003) “Technological Development in Indian Banking Sector”, Indian Streams Research Journal, Vol. 1, No. 9, pp. 1-4

[36] Schneider, G. (2002), “Electronic Commerce”, Thomson, pp. 183-201

[37] Singh P., Rao and Maheshwari (2005), “ A framework for evaluating E-Business Models and Productivity Analysis for Banking Sector in India”, International Journal of Internet Banking and Commerce, Vol. 10, No. 2, pp. 78-91

[38] Sohani, A. (2009), “Technology and Banking Sector”, ICFAI University Press, pp. 1-39

[39] Thornton J. and White (2001), “Customer Orientation and Usage of Financial Distribution Channels”, Journal of Services Marketing, Vol. 15, No. 3, pp. 168-185

[40] Turban, E. et al (2006), “Electronic Commerce: A Managerial Perspective”, Prentice Hall, pp. 129-156

[41] Taylor, M. and Murphy, A. (2004), “ SMEs and E-Business”, Journal of Small Business and Enterprise Development, Vol. 11, No. 3, pp. 280-289

[42] Uppal, R. (2011), “Indian Banking: In Age of Hi-Tech Area”, Lachoo Management Journal, Vol. 2, No. 1, pp. 54-69

[43] Velmurugan Manivannan Senthil (2009), “Security and Trust in E-Business: Problems and Prospects”, International Journal of Electronic Business Management, Vol. 7, No. 3, pp. 151-158

[44] Vijay Kumbhar (2011), “Customers’ Demographic Profile and Satisfaction in E-Banking Services: A Study of Indian Banks”, International Journal for Business, Strategy and Management, Vol. 1, No. 1, pp. 1-9

[45] Vivek Sharma, Rajiv Sharma (2000), “Developing E-Commerce Sites: An Integrated Approach”, Addison-Wesley, pp. 268

[46] Wang, Y. S., Y. M. Wang, H. H. Lin, and T. I. Tang (2003), “Determinants of User Acceptance of Internet Banking: an Empirical Study”, International Journal of Service Industry Management, Vol. 14, No. 5, pp. 501-519

[47] Windrum, Paul & De Berranger, Pascale (2002), “The Adoption of E-Business by SMES“, Journal of Economics, Vol. 108, No. 3 pp. 1-32

[48] Zwass, V. (2003), ”Electronic Commerce and Organizational Innovation: Aspects and Opportunities “, International Journal of Electronic Commerce, Vol. 7, No. 3, pp. 7-37