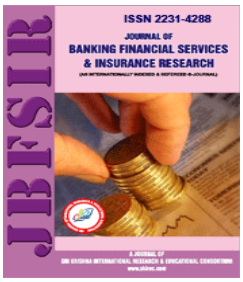
The Journal of Sri Krishna Research & Educational Consortium

JOURNAL ON BANKING FINANCIAL SERVICES & INSURANCE RESEARCH

Internationally Indexed & Listed Referred e-Journal



SECURE FINANCIAL SERVICES
(NEXT GENERATION CHALLENGE)

SHRISH KUMAR TIWARI

Shrish Kumar Tiwari, Research-scholar in Department of
Commerce and Business Administration,
University of Allahabad, Allahabad.

ABSTRACT

"PUT NOT YOUR TRUST IN MONEY, BUT PUT YOUR MONEY IN TRUST".

The recent economic crisis has resulted not only in serious challenges to, but also significant transformation in, the financial services industry. The financial turmoil - along with the increasing complexity of the financial ecosystem - has placed unprecedented and new demands on financial services institutions. Yet severe market disruption and dislocation also present an opportunity for institutions to drive innovation, differentiate products and services and break away from the competition.

Technology advances, regulatory changes, demographic shifts, and mobile lifestyles and work styles revolution are all factors likely to significantly reshape the financial services landscape in the next decade. By indentifying some of the timely and key trends for the industry, financial institutions can prepare and look at ways to turn adverse market conditions into profitable business opportunities. Information security is one of major cause of concern for the banks to maintain secure, robust and convenient financial system. Unfortunately this sector is not as secure as it be Everyday a new security challenge has arrives and increase the existing risk level of this sector.

This paper attempts to identify the various information security risks which can negatively affect financial sector in terms of information security .This paper also attempts to provide certain measure to make information much secure and robust.

INTRODUCTION

"The mantra of any good security engineer is: **'Security is a not a product, but a process.'** It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together. "— Bruce Schneier

As the macroeconomic environment begins to stabilize somewhat, financial services institutions are shifting their focus from survival to growth. Financial sectors are now seeing significant interest in consolidation, rationalization, and virtualization as financial organizations strive to become more effective and more adaptable businesses. Investment in IT and communication systems continues to contribute greatly to an agile and flexible operating model. However, IT innovation and delivery of 'IT as a Service' still involves challenges; not least in the legacy modernization and siloed infrastructures. Organizations are striving to match technology with fast changing business needs, but IT complexity remains the norm for most organizations.

Besides this banking sector is has been witness of rapid technological changes in the process of its operations inside and outside the bank. Things are converting in digital form i.e. Sim card, Credit card, ATM, etc. All these can be mention as the reasons for phenomenal growth of banking services in India. Traditional mode to operate banking has transformed by e-banking, m-banking model and contributing remarkably in customer convenience. From these technological evaluations where customers are benefiting, that they are assessing their bank any time, anywhere, other hand this system is suffering from a serious threat issue that is information security. Information is at the heart of today's business.

METHODOLOGY:

The present study is based on discussions with the information security experts and the secondary data are gathered from various reports (Information security reports, survey) and from various official website of responsible authorities and bodies .Data presented in this paper contains authenticity and reliability.

Objectives:

This paper is based on certain objectives which are as follows-

1. To identify the various security threats related to information of Indian Banks.

2. To analyse the awareness and approaches of banks regarding data protection.

3. To provide certain measures to overcome security risks regarding data protection in form of suggestions.

Technology has been one of the most significant drivers of the recent developments in the world of banking and finance. The use of technology in India has undergone rapid transformation with the last two decades witnessing a sea change in the nature of services offered by not only banks but also the financial sector and even the Government - all of which have had a positive impact on the customers of these organizations and the general public at large. The banks have also undergone a massive change in terms of improvement in the IT Communication network. The electronic banking service channels like ATM Applications, phone banking, Internet Banking Mobile Banking and cards have become important vehicles of offering banking services in a Cost-efficient manner with wide geographical spread. Since Electronic Banking is a new technology that has many capabilities and also many potential problems, users are hesitant to use the system. The use of Electronic Banking has brought many concerns from different stake-holders viz., government, businesses, banks, individuals and technology. But everybody's primary concern is the security.

Information security is all about protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Banks and other financial institutions amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored in electronic form in computers and transmitted across networks to other computers. When we discus about information security anywhere it primarily meant to **Confidentiality, Integrity and Availability** of network, system and information stored and used by banks and their customers.

CONFIDENTIALITY

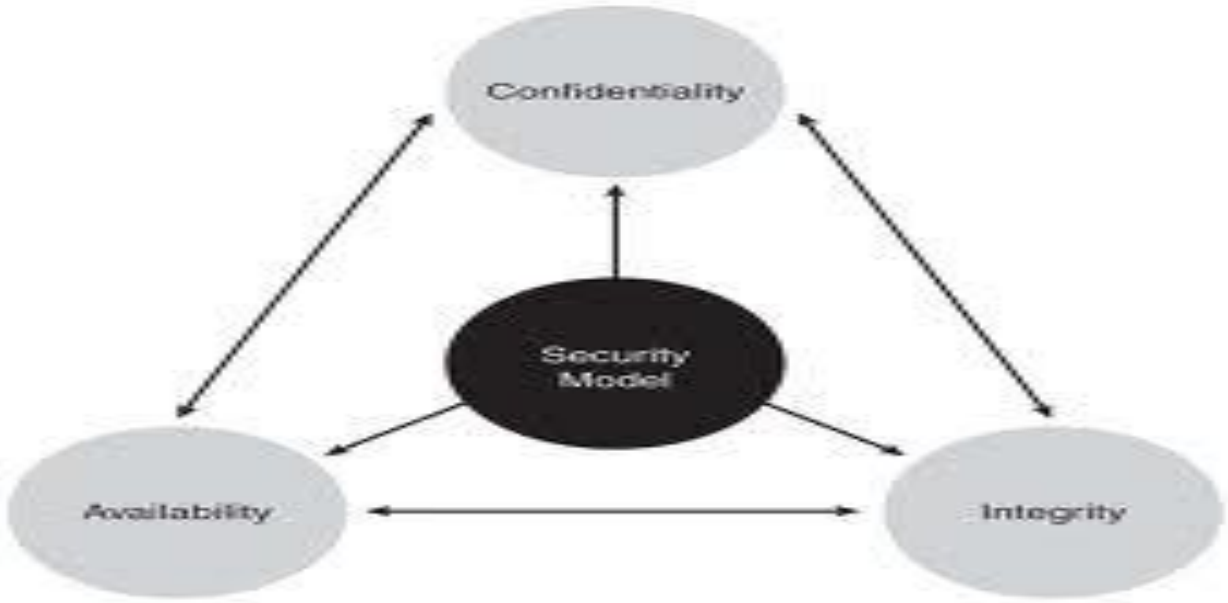
Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

INTEGRITY

In information security, integrity means that data cannot be modified undetectably. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

AVAILABILITY

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.



WHY SECURITY IS BIG DEAL?

Banks and financial institutions are the place where customer don't keep their money only but also trust that their wealth will safe .This is a unwritten agreement between banks and their customers based on trust and mutual understanding. AS more and more people join this new and emerging form of operating banking the responsibility of banks regarding provide secure transactions .In present technological era it's not possible for any banks to sustain in this highly competitive sector without using technology. Various studies shows that various big corporate houses are not showing their trust in system of India as for information security is concern and maintaining their data base outside of India. It shows that how our information security system is suffering from lack of trust. Although the situation is marginally better than it was a few years

ago, 55% of Indian corporates have little faith in the e-security apparatus of the country, and feel more comfortable storing sensitive IT data on servers abroad

THE KEY DRIVERS THOSE ARE LIKELY TO SHAPE FINANCIAL SERVICES DELIVERY THIS COMING DECADE:

1. TRANSACTIONAL SELF-SERVICE WILL BECOME THE NORM:

Mobile, online, and telephone banking channels will become channels of choice for personal banking. Branch network use will significantly shift towards advisory services – through both digital and human interactions. ATMs will morph into localized and mobile shared digital commerce kiosks and there will be an increased adoption of shared commerce kiosk provider networks

2. THE NETWORK WILL BECOME THE BUSINESS INFRASTRUCTURE PLATFORM

The network will no longer be viewed as a commodity. Security, identity, and IT services currently deployed at the network edge will increasingly migrate into the cloud. With embedded security, identity, intelligence, scalability, and resiliency, the network will become a strategic business infrastructure platform over which business and technology services delivery will be orchestrated locally, nationally and globally.

3. INFORMATION SECURITY WILL BECOME INCREASINGLY RISK-DRIVEN AND MEASURABLE

Cyber threats will become less and less risky as the decade unfolds. With stronger and more ubiquitous measures in place, we will see a significant decrease in e-mail spam, identity theft and much of the computer crime as we know it today. And those cyber attacks that continue will change in character to fewer, but more targeted attacks.

4. SOURCING MODELS WILL BE REDEFINED

Passionate debate around outsourcing (to outsource or not) will become increasingly less important. As business, commerce, and organizations become increasingly digital, virtual, and service-based, the discourse will shift to consistent and verifiable controls across an extended digital virtual financial enterprise regardless of who or where the work is performed.

5. 'EVERYTHING AS A SERVICE (EAAS)' IT AND INFORMATION ARCHITECTURES WILL DELIVER EFFICIENCY DIVIDENDS

Compliance, risk, and transparency initiatives will command significant share of resources and will weigh on efficiency. Financial institutions will however still show meaningful improvement in efficiency ratios as digitization, virtualization, standardization, and flexible services-oriented cloud architectures are increasingly adopted to drive business growth. This cloud-based delivery approach is much more than a fad, however – it has the potential to drive new waves of technology innovation, quickly and effectively open new markets, and essentially enable business strategies that help organizations practice better financial management and create a more sustainable model for the delivery of future IT services.

Essentially, underpinning all of these trends, are innovative business and technology solutions and services that will enable financial services organizations to compete (and comply) more effectively in the global market-place. They need a strong, secure IT and communications foundation that will enable business infrastructures and services to support the radical changes to business models that the markets, governments and customers will demand.

The bottom line is that these significant business challenges can only be effectively addressed through innovation in IT delivery models and reinvention of technology, and information architectures that enable on demand business, any time, any where, and on any device.

6. CONSUMER TRUST IN ONLINE MECHANISM

The development of electronic commerce is characterized with anonymity, uncertainty, lack of control and potential opportunism. Therefore, the success of electronic commerce significantly depends on providing security and privacy for its consumers' sensitive personal data. Consumers' lack of acceptance in electronic commerce adoption today is not merely due to the concern on security and privacy of their personal data, but also lack of trust and reliability of Web vendors, Consumers' trust in online transactions is crucial for the continuous growth and development of electronic commerce. Since Business to Consumer (B2C) e-commerce requires the consumers to engage the technologies, the consumers face a variety of security risks.

7. OUTSOURCING IT RISK

Firms face pressure to outsource to remain competitive with the cost base and head count migrating offshore. Outsourcing activities such as IT Development, Operations and Contact functions (e.g. call centers) , allows firms to build operational efficiencies, react and be flexible to competitive pressures and to provide organizational resilience. When outsourcing, a firm has to balance the cost savings realized with the operational risks taken in terms of the outsourced staff, processes and technology. A wide range of outsourcing practices was evident in the firms we visited – from no outsourcing to extensive outsourcing. Experience of outsourcing and off shoring varied – with one firm inheriting a subsidiary's outsourced function and only assigning it

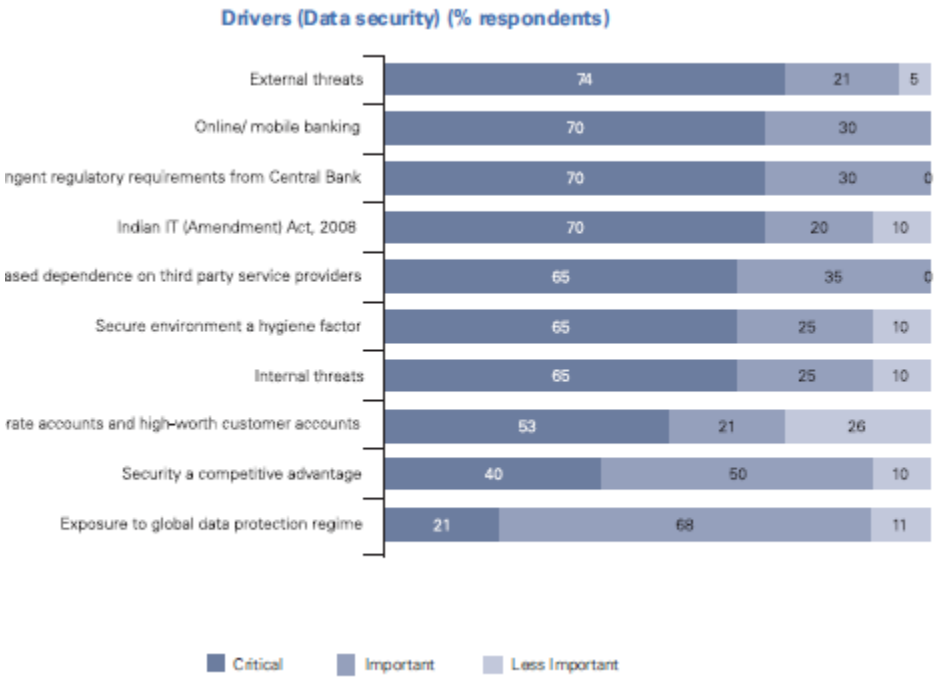
low-risk work, while another firm was embracing outsourcing by expanding its offshore operations with a new call centre function.

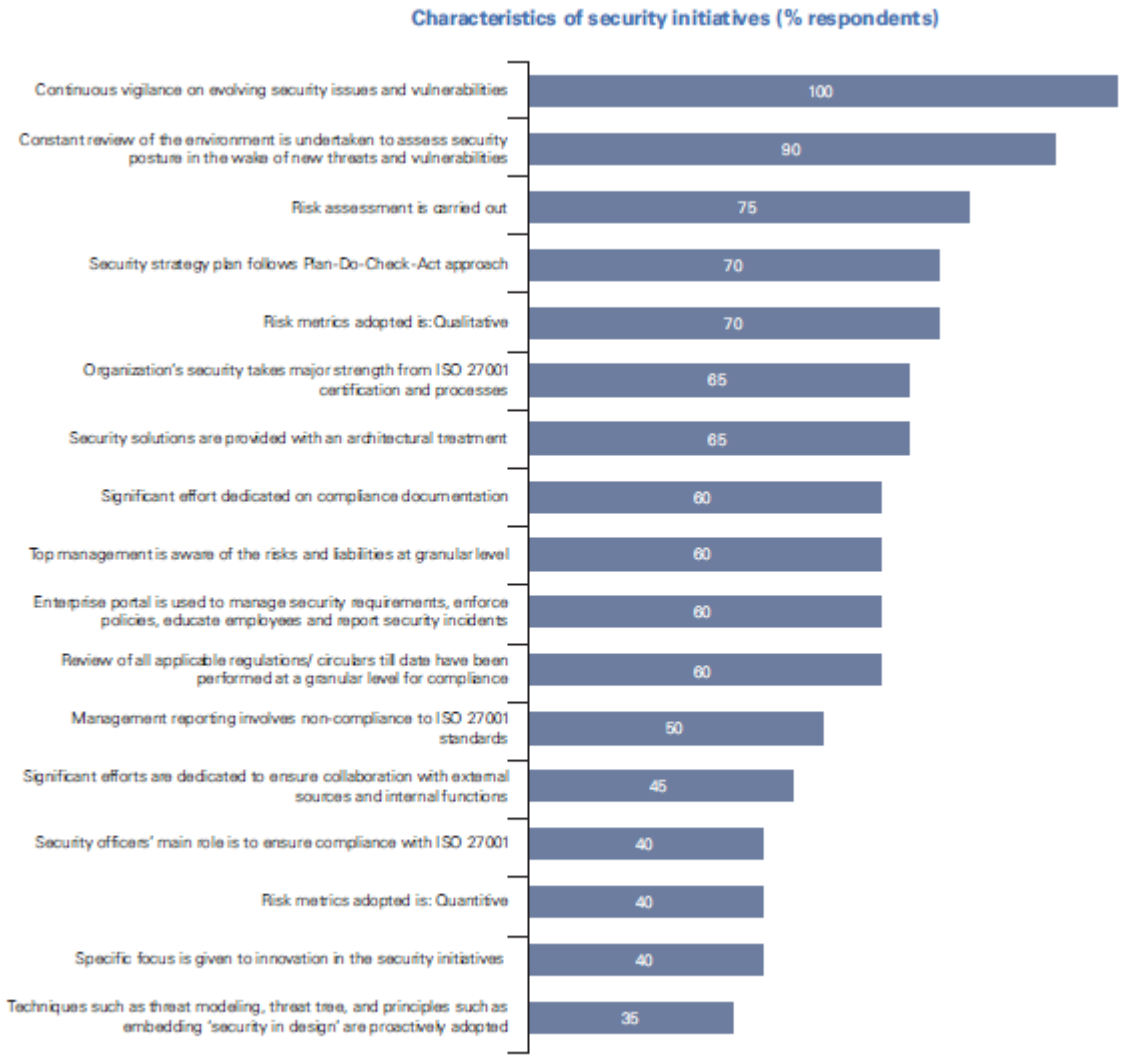
MAJOR INFORMATION THREATS:

As we discussed above that CIA model is the pillar of information security in any organization. By analyzing various security threats it has been observed that almost all threats are directly or indirectly associated on CIA (Confidentiality, Integrity, and Availability). Data stored within and outside the banks are not just few data but asset now a days when everything getting digital. So security of data is a crucial concern. Some Indian banks do not use up-to-date e-security solutions and are not spending much to ensure their data is not breached or stolen.

Correct Data Protection Mechanism:

Data thieves are highly sophisticated and grow more so every day. Their game changes constantly, with new technologies and new strategies. To keep up with them, government and business leaders will have to change their own game how to protect data outside an organization's four walls, how to build a culture for data protection, how to manage internal threats and how to collaborate to combat operational data theft.





Some major concern for data protection are as follows:

A. THIRD PARTY DATA EXCHANGE: PROTECTING DATA BEYOND FOUR WALLS.

Data that passes into the hands of a third party provider must remain as safe as it would be behind the firewall of the primary owner of the data. To achieve this, the primary owner must conduct risk assessments, carefully structure its contract with the third party, continually audit the third party's compliance and develop a detailed action plan for dealing with third party breaches. Know the risks of doing business with third parties.

B. BUILDING A CULTURE FOR DATA PROTECTION

A agency must develop a culture in which each individual appreciates the importance of data security and takes personal responsibility for maintaining it. Top executives must lead this effort and reinforce it through the compensation structure. Data is the most valuable asset; it is everyone's personal responsibility

C. INSIDER THREAT: THE THREAT WITHIN YOUR WALLS

Complacency is a major obstacle to vigilance. Just because nothing has gone wrong yet doesn't mean nothing will. People change. The employee who proved trustworthy last year might have suffered a crisis since then that increases the emptation to betray an organization's trust.

D. OPERATIONAL FRAUD: A NEW COLLABORATIVE APPROACH TO DETECTING FRAUD AND MINIMIZING THE IMPACT

Facing inward, an organization needs an enterprise risk management strategy, bringing together all the domains that deal with security (fraud prevention, loss prevention, network security, etc.) to attack the problem in an integrated fashion. Facing outward, different public and private sector organizations must establish rules of engagement for exchanging actionable information, so they can collaborate against common threats. Success demands the right combination of tactics, tools and collaboration. Fusing data and performing analysis from multiple information sources can provide relevant insight and allow an organization to discover inappropriate activities.

SUGGESTIONS:

"we need courage to throw away old garments which have had their day and no longer fit the requirements of the new generation"

Its also very true for security also. Technology is changing very fast but our counter measure for checking vurnbilities, threats ,and various other fraud is not as update and fast .Hence cyber criminals, intruders are creating various challenges before our economy .Our any step solve one problems but new day comes with new danger,again same process. So there must be a long time policy to maintain a secure,and robust information system . Following measures may be helpfuil for this-

Nine Point Approach for securing the Data in organization

1. Conduct an inventory of data and limit access to it.
2. Set up a credentialing program for employees, customers and vendors.
3. Establish corporate accountability, starting at the highest levels of the organization.
4. Execute standards, procedures and guidelines.

5. Use a third party to audit whether everyone is complying correctly with data security policies.
6. Keep investigating new technology solutions to help enforce your policies.
7. Provide mandatory training programs for employees and customers.
8. Conduct education and outreach, targeted internally to your organization and externally to stakeholders.
9. Maintain transparency in everything you do.

Apart from above one creation of awareness among related parties-customer, banks, and other associated bodies, is inevitable need to maintain secure financial system. Our judiciary ,administration, and police should be tech savvy and skilled to counter with these non-traditional types of crime .

CONCLUSION:

"Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds. "

It's not an easy task even for the Government to maintain full proof security system to protect information. This is responsibilities of all concerning parties to know the importance of their information and try to keep secure this from strangers because they know the importance of your information may be you not but they .

So a holistic approach is required to maintain security and to create trust in customers mind regarding banking and security.

REFERENCES:

http://www.availability.com/resource/pdfs/DPRO-100862.pdf

http://www.collectionscreditrisk.com/news/quarterly-merger-activity-see-saws-despite-upward-trend-3005962-1.html?ET=ccrisk:e5846:58284a:&st=email&utm_source=editorial&utm_medium=email&utm_campaign=CCR_breakingnews_042611_042611

http://www.dnaindia.com/mumbai/report_over-half-of-indian-firms-store-digital-data-abroad_153723

www.iba.org.in/events/Inaugural%20Address.pdf

www.iba.org

www.cert.in

http://www.nativeintelligence.com/ni-free/itsec-quips-03.asp

Kumar Abhay, Information Security Policy & Regulation Issues

Sharma K.K., Responsive Administration of the criminal justice system in India, special number on Towards Good Governance: initiatives in India, Prentice- hall of India, New Delhi

Sharma Vakul, E-governance & Information Technology Act ,2000(book name is Information Technology Law and Practice cyber law & e-commerce) Universal law publishing Co. Pvt. Ltd.
Chip Magazine. 'Special Edition'. Mumbai
Official Website of NASSCOM
Official Website of APIAP
Cyber Crime Cell, Mumbai PHISHING.mht

file:///C:/Documents%20and%20Settings/sai/Local%20Settings/Temp/Temporary%20Directory%201%20for%20cyberterrorism.zip/CYBER%20TERRORISM%20AND%20ITS%20SOLUTIONS%20AN%20INDIAN%20PERSPECTIVE.htm
https://secure.infragard-ct.org/.../harold_hendershot_02092003

www.allvoices.com/...india...check-cyber-terrorism/stories - United States

"INDIA NOT READY FOR CYBERWAR" Business Standard (Lucknow edition) February 4th, 2010, pg.11.

"Moiley for special law to tackle cyber crimes" business standard (Lucknow edition) February 1st, 2010, pg.6

Berger, A.N. and D.B.Humphrey (1997), 'Efficiency of Financial Institutions: International Survey and Directions for Future Research', *European Journal of Operational Research*, 98, pp. 175-212.

Berger, A.N. and R De Young (1997), 'Problem Loans and the Cost Efficiency of Commercial Banks'.

Journal of Banking and Finance, Vol. 21, pp. 841-870.

Bauer, P.W., A. Berger, G.D.Ferrier and D.B.Humphrey (1998), 'Consistency Conditions for Regulatory Analysis of Financial Institutions: A Comparison of Frontier Efficiency Methods', *Journal of Economics and Business*, 50, pp. 85-114.

Das Abhiman (1997), 'Technical, Allocative and Scale Efficiency of Public Sector Banks in India', Reserve Bank of India Occasional Papers, Vol.18 No:2/3 June-September.

Fecher, F. and P. Pestieau, (1993), 'Efficiency and Competition in OECD Financial Services' in "*The Measurement of productive efficiency; Techinques and Applications*." edited by H.O. Fried, C.A. K.

Lovell and S.S. Schmidt Oxford University Press, New York, PP 374-385.

Pastor, J F. Perez and J. Quesada (1997), 'Efficiency Analysis in Banking Firms: An International Comparison', *European Journal of Operational Research*, 98, pp. 396-408.

Bank for International Settlements (1999), '*Bank Restructuring in Practice*', BIS Policy Papers.

Government of India (2000), *'Budget for 2000-20001',* Speech of Shri Yashwant Sinha, Minister of Finance, February.

Goldstein Morris and Phillip Turner (1996), *'Banking Crises in Emerging Economies: Origins and Policy Options*', BIS Economic Papers No.46, October.

Goldstein Morris (1997), *'The Case for an International Banking'*, Institute for International Economics, April.