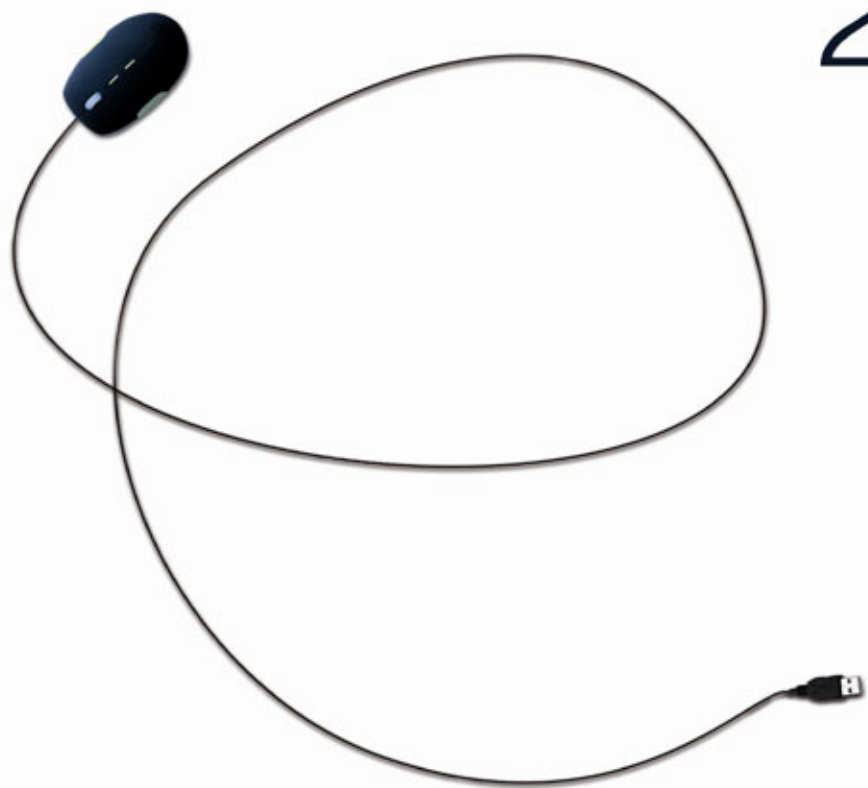


2^e



e-finance

the future is here

V C JOSHI



E-finance

E-finance

The future is here

Second Edition

V.C. Joshi



Response

Business books from SAGE

Los Angeles ■ London ■ New Delhi ■ Singapore ■ Washington DC

www.sagepublications.com

Copyright © V.C. Joshi, 2010

All rights reserved. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage or retrieval system, without permission in writing from the publisher.

First published in 2004

This second edition published in 2010 by



Response Books

Business books from SAGE

B1/I-1 Mohan Cooperative Industrial Area

Mathura Road, New Delhi 110 044, India

SAGE Publications Inc

2455 Teller Road

Thousand Oaks, California 91320, USA

SAGE Publications Ltd

1 Oliver's Yard, 55 City Road

London EC1Y 1SP, United Kingdom

SAGE Publications Asia-Pacific Pte Ltd

33 Pekin Street

#02-01 Far East Square

Singapore 048763

Published by Vivek Mehra for Response Books typeset in 10/12pt Bembo by Star Compugraphics Private Limited, Delhi and printed at Chaman Enterprises, New Delhi.

Library of Congress Cataloging-in-Publication Data

Joshi, Vasant C., 1932–

E-finance: the future is here/V.C. Joshi—2nd ed.

p. cm.

Includes bibliographical references and index.

1. Financial services industry—Computer networks—India. 2. Internet banking—India. I. Title. II. Title: E-finance.

HG187.I4J68

332.10285'4678—dc22

2009

2009044224

ISBN: 978-81-321-0245-8 (PB)

The SAGE Team: Reema Singhal, Sushmita Banerjee and Trinankur Banerjee

About the Author

V.C. Joshi is a financial services consultant based in Pune. He retired as General Manager UK and European branches, Bank of India and had served as a Director of the National Insurance Academy, Pune, India.

He has also served on important committees and on the boards of several organizations. He was Chairman of Indian Banks' Association, London. He has also worked as a consultant in India with PriceWaterhouse Coopers and has been a guest faculty at various institutions, including the Bankers' Training College (RBI) and the National Institute of Bank Management.

He has authored several books, including *Managing Indian Banks: The Challenges Ahead* (third edition, 2009), and numerous articles in the areas of banking and finance.

Contents

<i>List of Tables</i>	ix
<i>List of Figures</i>	xi
<i>Preface</i>	xiii
1. Indian Developments within the Global Context	1
2. E-finance Delivery Channels: Impact on the Bottom Line	10
3. Websites	17
4. Products and Services in India	27
5. E-banking and E-insurance	37
6. E-trading	63
7. Click and Brick Marketing	74
8. General Aspects of Risk Management	90
9. Risk Management for E-banking and E-insurance	104
10. Cyber Crimes	111
11. Network Security	118
12. Cyber Laws	141
13. Regulation of E-finance Institutions	159
14. The Internet Potential	174
<i>Bibliography</i>	179
<i>Index</i>	184

List of Tables

1.1	Growth of Internet Users in India	2
1.2	Growth of Global Internet Users	2
5.1	Internet and Non-internet Banks—A Dynamic Analysis	56
5.2	Internet and Non-internet Banks—Selected Balance Sheet Ratios <i>(a)</i> Loan Comp. <i>(b)</i> Funding	56
10.1	Cyber Crimes and Their Effect	114
13.1	New Ways of Paying On-line	169

List of Figures

5.1	Product Complexity	60
5.2	Pre-internet: Insurance	61
5.3	Internet-enabled Insurance	62
7.1	Customer Service	76
7.2	Marketing Plan in Corporate Plans	79
7.3	Supplier Reach	83
8.1	Interrelations of Risks	91
9.1	Analysis of Risk	105

Preface

The preparation of the second edition of this book was a daunting task. The financial services industry is faced with problems as never before. It is unlikely that the banks/financial institutions would have the time or inclination to look at the issues of technology upgradation or actively marketing the channel and make it available at substantial costs. The paramount issue continues to be managing the crisis and its aftermath, and other issues were likely to be relegated to the background. But in all this, there is a ray of hope.

The Indian banks (particularly public sector banks) have not suffered; they are sound and considered quite safe too. This is almost a unique event because all these years our efforts at locating Indian banks in the first 200 banks in the Bankers' Almanac were in vain. But here is an opportunity to show to the world that this business model can be used sensibly and with a social purpose. The whole tenor of this edition is to see if technology can be put to use to show the investors that our banks/financial institutions can offer them services at competitive prices.

However, there are some doubts if the banks and the private sector service providers could rise to the occasion. We, as spectators of the banking scene, can see more of the game than the players themselves.

But the nagging questions cannot be wished away. The first and most obvious question is the role the private sector is likely to play in providing the infrastructure facilities. The doubts arise because the private sector seems to place excessive reliance on short-term gains and greed appears to be the driving force. Further, firms like Enron resort to all kinds of dubious practices and are ready to flout even the prevalent laws/regulations, and so on. However, the World Bank in its 2008 report on 'Global Economic Prospects—Technology Diffusion in the Developing World 2008' has asserted that 'in both low and middle-income countries, policy should place special emphasis on incentives and on maintaining strong

ties to private-sector firms'. In view of the somewhat dubious record of the private sector firms, one has to await the policy issues and decisions regarding the same before delving further into the other questions. There is reason to believe that the current policies in this behalf are likely to be in place for some time to come and that no major changes were in the offing in the near future.

At another level there is reason enough to plead for normalization (in the immediate aftermath of the crisis) of other aspects of functioning of banks/financial institutions and avoiding the organizational paralysis. It is likely that the crisis has an all-pervasive engulfing tendency and that the functionaries behave as if they have no time to carry out and overview the routine activities. The crisis can become an excuse for not undertaking these tasks or for neglecting them and thus creating a wrong impression that these routine tasks can wait. It is important to note that crisis resolution can never be an excuse for neglecting other important tasks.

There are equally important issues awaiting resolution. Banks/financial institutions have invested huge amounts on creating the infrastructure and integrating the new channels is a very important task. It can be neglected only at a great cost. Further, even a slight relaxation of controls has the potential of inducing frauds and illegal transfers. Every effort has to be made to see that no laxity prevails and that the 'operational risks' management is not neglected.

In the last five years many Indian banks have started offering these facilities to their customers and even some medium-sized cooperative banks are venturing forth into adopting core banking solutions with the promise of migrating to the internet. In this book we would briefly touch on the issues like web designing but the emphasis would be on integrating the new channel with the established 'brick/click' model. The first chapter deals with the spread of the internet facilities and the use of mobile phones with internet connectivity. Next, we look at the economic basis for important decisions like pricing, price discrimination and marketing of services. It is necessary to look at other changes in routine administration, particularly back office functioning. The Financial Services Authority in the UK has been for sometime advising banks about dangers lurking round the corner. The range of products and services offered has gone up but with one major constraint. At one time, major banks were considering the possibilities of turning themselves into investment banks. They had quite clearly decided to avoid forays into retail banking. The situation regarding hedge funds and the future options was not very clear when this book was being written. This book also looks at the workings of e-banking, e-insurance and

e-broking. The developments in alternate systems of trading in areas like treasuries and foreign exchange have been discussed. The security aspects and the legal means available for dealing with crimes are critically looked at. Marketing of these services is a comparatively neglected area and recent experiences and efforts of some banks are looked at, to see if similar business models are applicable. Finally, the most difficult issues relating to regulation needs to be resolved. The wider questions about the shape of the future were and are still hazy. How specific issues would be resolved at the global level remain unanswered. Instead of making guesses or hazarding suggestions, we contend ourselves with what is and what currently determines the contours for operations.

Preparation of a work like this in the present context is extremely difficult. On the one hand, we witness the spectacle of reputed institutions falling like nine pins and on the other, fundamental questions pertain to what does the future hold for us. One has to tread a very difficult path and had it not been for the generosity of friends and erstwhile colleagues, it would never have been possible for me to complete the task. I would never be able to repay this deep debt of gratitude I owe to a host of friends. Even though I have mentioned only a few names here, the others have also made equally valuable contribution to this endeavour. P.B. Kulkarni, former CMD of Bank of Maharashtra; Suhas Bhat, CMD of Indian Overseas Bank and Dilip Patwardhan, General Manager, Bank of India were at all times ready to answer my queries, read sections which I thought needed some careful attention and always made it a point to supply papers, articles and book reviews which had a bearing on our work. I would be failing in my duty if I failed to express my sincere and grateful thanks to Shrikant Sarpotdar for his help in clarifying a number of points related to risk management, accounting policies and other related matters. His constant encouragement was an important factor in spurring me on to greater efforts.

The editorial teams at SAGE have always been extremely supportive and are ever willing to take on our behalf, responsibilities which may not strictly fall within their domain. Our special thanks are due to Dr Sugata Ghosh, Reema Singhal, Sushmita Banerjee and Payal Kumar and her team of dedicated editors for their valuable contribution. Thanks is too mild a word to express all that I feel within.

Last, special thanks are due to my wife who patiently and silently carried out myriad tasks to ensure that the household ran like a well oiled machine and I was not even made aware of the difficulties she had in managing the daily chores. She additionally gave valued support through

encouragement and at times even prodding with a persistence which drew me again and again to the drawing board. My son Vinay deserves a special mention. Getting drafts approved by him is an arduous task and had it not been for his valued comments, there would have been innumerable gaps and even errors. It is very difficult to repay this deep debt. My son-in-law Kirtikumar Deshpade, daughter Achala Deshpande and my grandson Sameer Deshpande made valuable suggestions, allowed me to draw on their computing skills and helped in myriad ways in supplementing my unskilled efforts.

I hope that the banks would use the approaches mentioned in this book not only to woo customers overseas and but also to retain them. Such opportunities are not likely to be there over and over again. Our hands are nowhere near the rudder and all that we could do is cry out loudly and clearly, and show the way ahead. The future is here. May FIs exploit it!

V.C. Joshi

Indian Developments within the Global Context

About five years ago, when the first edition of the book came out, the dot com bust had cast its long shadow over the internet developments. One was somewhat hesitant about the wide spread acceptance of this medium. However, the last five years have dispelled whatever doubts one may have had about its usage. The financial services industry in particular has witnessed major shifts in customer preferences in the use of this channel and security concerns notwithstanding, there is a tremendous growth in its use.

This chapter begins with a review of the global growth in internet usage. This is followed by a discussion on impact assessment and return on investment. We have devoted a separate chapter to review what is now described as 'Internet Economics'. This chapter broadly examines the usage and the impact of internet on the financial services industry in general.

The internet is a multipurpose and multipoint, digital, interactive, world-wide telecommunications network. By its nature, internet facilitates multipoint information flows and all the processes that are based on information flows. Financial intermediation and financial exchanges are based on the exchange of information. In fact, at present, a transaction of exchange of financial instruments, including equities bonds and their derivatives, is just a record of altered digital information.

It is not possible to better President Clinton's description of the way the internet has grown during the last few years. 'When I took office, only the high energy physicists had ever heard of what is called World Wide Web. Now even my cat has its own page.' The internet grows almost day by day.

2 E-finance

THE INTERNET EVOLUTION

The growth of internet usage in India from December 1995 to June 2007 has been reviewed in the following paragraphs. Tables 1.1 and 1.2 provide the statistics for usage in India and the growth of global internet users respectively.

Table 1.1 Growth of Internet Users in India

<i>Year</i>	<i>Claimed Internet Users (in million)</i>	<i>Active Internet Users (in million)</i>
2000	4.9	2.2
2001	8.7	4.3
2002		
2003	11.9	7.5
2004	16.4	11.2
2005		
2006	32.2	21.1
2007	46	32

Source: <http://www.iamai.in/Upload/Research/I-Cube-2007-Summary-Report-final.pdf>

Table 1.2 Growth of Global Internet Users

<i>Date</i>	<i>Number of Users (in million)</i>	<i>World Population (in %)</i>	<i>Information Source</i>
December 1995	16	0.4	Industrial Development Corporation (IDC)
December 1996	36	0.9	IDC
December 1997	70	1.7	IDC
December 1998	147	3.6	C.I. Almanac
December 1999	248	4.1	Nua Ltd
December 2000	361	5.8	Internet World Stats
August 2001	513	8.6	Nua Ltd
September 2002	587	9.4	Internet World Stats
December 2003	719	11.1	Internet World Stats
December 2004	817	12.7	Internet World Stats
December 2005	1,018	15.7	Internet World Stats
December 2006	1,093	16.7	Internet World Stats
December 2007	1,319	20.0	Internet World Stats
December 2008	1,574	23.5	Internet World Stats
March 2009	1,596	23.8	Internet World Stats

Source: <http://www.internetworldstats.com/emarketing.htm>

There are other reports about usage in India from JuxtConsult. The research offers insightful, comprehensive and up-to-date understanding of net usage behaviour and online preferences of regular internet users. India Online 2008 understands online Indians as consumers and not just faceless net users. It has been a year of healthy growth in the Indian online space. The number of internet users could well be put at about 49 million. Of these about 40 million are urban users while about 9 million are in the rural category. The growth in the number of regular users is very substantial at 33 per cent. It might be useful to add that 'regular' refers to accessing the net at least once every month.

Growth has been both in class and in mass of online users in India. Seventy-seven per cent of all online users belong to the 19–35 age group category, 70 per cent of the total users belong to the large, medium- and small-sized towns and townships, 51 per cent users are salaried employees, 63 per cent users own an automobile and English is the most preferred language of reading for only 28 per cent of internet users (indicating the potential for vernacular language content).

For some time now it is becoming increasingly customary to compare the growth in such sectors in China while looking at the Indian figures. China's fast-growing population of internet users has soared to 221 million, tying the United States for the largest number of people online, according to government data reported in the last three years. The figure, reported by the Xinhua News Agency, reflects China's explosive growth in internet use despite the government's efforts to block access to material considered subversive or pornographic. It was a 61 per cent increase over the 137 million internet users reported by the government at the start of 2007. China lags the United States, South Korea and other markets in online commerce and other financial measures. But e-commerce, video-sharing and other businesses are growing quickly and companies have raised millions of dollars from investors.

'We'll see this growth continuing,' said Duncan Clark, chairman of BDA China Ltd. These figures speak for themselves. Apart from the numerical differences there is a distinct possibility that this network capacity would soon be put to use to promote Chinese trade and commercial activities particularly in the small- and medium-sized enterprises.

Earlier the fear that the rural–urban divide may be glossed over or completely ignored, has to some extent been overcome by the establishment of internet cafés, which provide facilities for internet usage and these need to be taken into account when looking at the number of connections. It is true that merely having these facilities does not automatically lead to the

4 E-finance

conclusion that this has some correlation with internet trading or that these facilities are used for financial transactions. Books like Friedman's *World is Flat* create an impression that the transition to internet trade has already been made or that it is just round the corner. It is not quite correct. One must remember that barely 26 per cent of the total population in India has any relationship with banks as such. Only 19 per cent of them have, perhaps, access to loan facilities. It is, therefore, quite clear that the use of the internet in financial transactions is restricted to the more technology savvy clients. We, however, feel that mobile telephones may facilitate some primary banking functions. With the help of mobile phones and internet, queries regarding account balance can be sent or bills can be paid. However, much would depend on the pace of technical developments.

Before analysing the impact of net-based services on the financial services industry, it must be added that the security concerns and very tardy pace of getting legal remedial action has deterred many prospective users. In addition, one faces the difficulty about having precise information about the use or periodicity, expenses incurred, and so on. Therefore we would have to use parallels from other countries and then try and see to what extent these might be applicable in the Indian context.

Before proceeding to an impact assessment exercise, it is necessary to highlight the peculiar characteristics of the internet.

- It is a single worldwide communication network.
- It offers instant up to the minute access to information.
- It has the ability to transform massive amounts of data online.
- There is an army of developers refining and creating applications that make access easier.
- It is a vast source for global information regarding stock prices, exchange rates and thousand and one other details. These could determine risk levels for critical investments.
- The speed and accuracy could be described as the special features of this delivery channel.

Instead of dealing with the subject in the abstract, we can give it a more concrete shape. Capital is managed around the clock in globally integrated financial markets in real time. Billions of dollars worth of transactions take place in seconds in the electronic circuits throughout the globe. New technologies allow capital to be shuttled back and forth between economies in a very short time. Capital and, subsequently, savings and investments are

interconnected worldwide from banks to pension funds, stock exchanges to currency exchanges.

IMPACT ASSESSMENT

One has to remember that we have an extremely potent and versatile tool, and it is up to the management to ensure its effective utilization.

It needs to be clarified at the outset that our approach to the problem is somewhat restricted. We do not intend to look to the wider questions like the effect it has on trade union problems or the impact on Indian economic policy or the way global capitalism is using the technology for a given purpose, and so on. To what extent the questions like growth of technology and changes in the means of production substantiate Marxian analysis are no doubt interesting, but are far from our current area of discourse. Those who would like to look at these and related issues could most profitably look at Castell's *The Rise of Network Society* (see Castell 2000).

This chapter does not examine the question in the light of earlier exaggerated hopes raised about the internet. It is true that in those days we were expecting the branch network of banks or of broking houses to shrink and, over a period, to wither away. Bill Gates' assertion that we need banking, but not branch banking has been belied. The current scenario has both the channels playing a very important role in the distribution of financial services. 'Brick and Click' is the order of the day.

This chapter is primarily concerned with questions that a bank/broking house management would ask before/after undertaking such investments. The decision to invest could have been made for various reasons. However, the management needs to know about the level of adoption of internet solutions and also needs to measure the impact on revenue and on costs. The focus to start with would be on broad business areas as well as keying on specific areas. The list could be somewhat as follows:

- Customer development and e-marketing.
- Customer service and support.
- Business-to-business (B2B) growth in activities.
- Finance and accounting (improvements due to centralization).
- Retail and wholesale operations.

The review of the planned areas of future developments is a must for such an exercise. Equally necessary would be a critical review of incomplete

6 E-finance

areas of work. Perhaps a review of investments done and the current market value of such investments will have to be part of the review exercise.

One must get a clear idea about the increase in revenue, decreased costs, decreased general expenses and/or operating expenses. In case of financial industry, a reduction in staff costs and, equally important, the per transaction cost, will have to be reviewed. Failure of expected financial impact of all internet business solutions will have to be reviewed against both tangible and intangible aspects of working.

The following list contains the areas that need special attention.

- Customer satisfaction.
- Workforce efficiency.
- Employee satisfaction.
- Revenue per customer.
- Customer acquisition costs.
- Customer retention costs.

It is important to quantify and critically evaluate the results. It is also important to review strategy changes. Sandra Sucher, lecturer at Harvard Business School, points out that, in general, banks have been slow to adopt technology and change their style of functioning.

The working of a very key department in a bank has been reviewed in the following paragraphs. The treasury is one of the major contributors to the bank's sound working. Their working has been affected by the fact that now telephone has been replaced by the internet.

- The internet has evolved to create information-rich websites that help in providing information about market rates and facilitating research directly to the clients.
- Market now demands customized rates and terms.
- There is cut-throat competition. Each supplier has unique products, unique attributes and alliances. This has resulted in reduced margins, disintermediation and entirely new client relationship management.
- Considerable transparency in area of fees and charges.

The changes have made it imperative for the treasury departments to be properly integrated with other operations. Treasury systems have to be internet-ready. This must result in improvements in the following areas.

- Forecasting quality.
- Global hedging of local payments.
- Reduction in duplicate entry of cross payments.
- Elimination of paper work to a large extent.

The question then is to bring the treasury systems developers, top management and others closely connected with this work to see that a proper integrated and coordinated system is in place.

The aforementioned analysis brings home one point: it is not the size of investment or even availability of latest technology, but a proper integrated approach in which various stakeholders contribute to successful implementation.

INTERNET FOR UNDERDEVELOPED COUNTRIES

A wider question that is often raised pertains to the possibility of the use of internet technology in underdeveloped countries. We are of the view that e-finance has great potential to improve the quality and scope of financial services, to expand opportunities for trading risks and widen the access to financial services for a much greater set of retail and commercial clients by offering more cost-effective delivery of services. Africa online and Bangladesh Grameen Bank experiences are the real pointers in this direction. One could certainly say that the ability of these countries to adopt the new internet technologies would depend on their telecommunication infrastructure. One would perhaps have to assert that the low efficiency and quality of financial services and the skewed profile of users favour migration towards e-finance. Online brokerage is a case in point. E-finance allows a much easier access to global capital and financial service providers.

Before coming to organization-specific questions, it is essential to deal with enabling factors and these, as has been stated previously, play an important part in the Indian context. India is amongst the few countries, which has taken significant steps in creating the required enabling environment. The factors listed here would make it quite easy for us to make the transition to e-finance:

- Regulatory framework for telecommunications.
- Security framework and public key infrastructure.
- Framework for information and privacy.

8 E-finance

- Framework for contract enforcement.
- Financial system laws.
- Market infrastructure.

The World Bank has come out with a system of ‘weights’ for some of these areas and we are listing the important ones.

Enabling Services and Their Importance

- Regulatory framework for telecommunication (very important).
- Security framework and public key infrastructure (very important).
- Framework for information and privacy (very important).
- Contract enforcement (very important).
- Market infrastructure (somewhat important).
- Consumer protection (very important).
- Investor protection (very important).
- Competition policy (very important).

REGULATORY FRAMEWORK FOR TELECOMMUNICATION

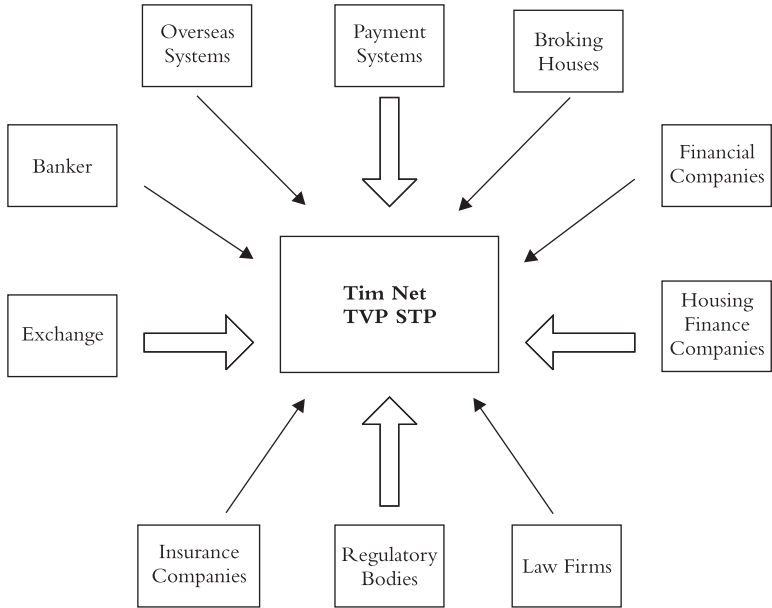
Telecommunication regulation is a key area for e-finance. Non-fixed lines are offering important possibilities in developing countries, including Africa, China and Cambodia. What is required is improvement in postal and telegraph administration, proper pricing regulations, and so on.

It would suffice to say that these factors, which would otherwise have hindered the developments, have in fact propelled the changes. Instead of relying on some benchmark figure like internet connectivity, it is better to look at the totality and decide on the possibilities.

One must at this stage try and predict what the future could hold for us. This is best described in the figure given in the appendix overleaf.

APPENDIX

What Does the Future Hold?



Source: Hong Kong Monetary Authority, quoted in Sitjin et al. (2000).

E-finance Delivery Channels: Impact on the Bottom Line

The last chapter highlighted that there are immense possibilities for Indian banks to seek and expand their customer base. The experience of the National Stock Exchange or the Clearing Corporation of India clearly highlights the fact that we now have an infrastructure in place which is second to none and that we could take advantage of the current difficulties faced by the financial sector in developed countries. In fact, some of the commentators are suggesting that Indian financial institutions do offer a safe and secure environment and that they would rank India as a secure and safe investment destination. However, financial institutions need to be careful and must make sure that in their zeal to take advantage of the present woes of developed nations, they do not tend to be complacent and that they take a hard look at their financials not only afterwards, but also prior to launching a marketing drive. Additionally, they would have to make major changes in their work systems and in the way the workforce responds to these challenges. Fortunately, the IT industry has shown the way world-class services can be offered through a sustained effort and more importantly, a vision.

This chapter begins with the question of return on internet investments. Banks and other financial service providers have invested large amounts of money on technology upgradation and the question assumes a considerable importance as we find that these aspects are not getting the attention they deserve. Next, we look at the specific economic aspects and try to assess the impact on the working of firms. How would it affect the working of the banks/broking firms is a question of great relevance in the context of

our approach to these problems. But this assessment is likely to overlook questions of unmeasured and often important gains to consumers from added convenience, wider product mix and customization that the internet makes possible. The following analysis will have to be viewed under the limitations listed here.

RETURN ON IT INVESTMENTS

There is a growing awareness that all IT expenditure does not automatically qualify for being described as sound investment. Returns on such investments and consequent improvements in productivity are being questioned. This chapter examines these arguments in some detail as these issues have not received the attention they deserve. Today, worldwide, billions of dollars are spent to support the requirements of the IT industry. However, even after this, many of these firms have shown little results. Unacceptably, a large percentage of the resources expended on IT by all manners of financial institutions, seem to disappear into a veritable black hole. A review of US government expenditure on software shows the extent of such misutilization. Forty-eight per cent of the software projects paid for never fructified. Of those delivered, 30 per cent are never used while 20 per cent are just abandoned. Only 2 per cent are ever used.

The firms that fall too far behind in the IT race stand to lose much more than their competitive advantage. The demise of many distinguished investment banks could, amongst other things, be attributed to the trade-processing systems not being up to the mark.

It must be emphasized that there is no substitute for active senior management support and involvement for IT investments to be beneficial. But certain questions which are far more serious than mere implementation aspects have been raised in the following page. The *Financial Times* in its IT review section (Wates 2003) puts forward the view that 'information technology systems have lost their way and may have failed to deliver what they promised to business. In the use of technology to transform business something has gone wrong'. Somewhere in the 1990s, amid the flowering of IT innovation, something seems to have gone wrong. One could list the following as the likely sources for the problem. The same is now true for the Indian financial institutions.

- The new computing technology (architecture) liberated users from the tyranny of the main frame, but exposed them to a failure of technology management.

12 E-finance

- The new client/server architecture transferred the power of its managers, who helped run the departmental processes smoothly. These managers tended to lose sight of the bigger picture.
- The new internet technology did not live alone. IT had to fit into a complex system. For some reason, when the internet came along, the pain of the past was forgotten.
- Components have developed rapidly but critical elements are lacking.
- Technology has not aligned itself with business management. The technology vendors blame the management and management blames the vendors. The fact is that there is a high rate of IT project failure.
- Low utilization of IT assets is another symptom of that malady. Its capacity utilization is barely 50 per cent.
- Last, one could refer to the high cost of maintenance of corporate information systems. 'The proportion of IT budgets in just keeping the lights on and the business running is far too high' (*Financial Times* 2003).

However, these are not insurmountable problems. The development of integrated systems and build-up of industry wide standards could be possible solutions. However, Nicholas Carr, *Harvard Business Review's* editor-at-large, has raised a still more fundamental issue relating to IT.

IS IT AN INFRASTRUCTURE TECHNOLOGY?

Carr (2003) notes that 5 per cent of the capital expenditure of American companies went on IT initially. In the 1980s, it rose to 15 per cent and by 1990 it had risen to 30 per cent (in India, too, we are witnessing the same trend. A number of banks here have announced the plans to spend crores of rupees on IT in the next couple of years). He further adds that there is a general belief that its potency has increased and that its strategic value has also gone up.

Carr (2003) questions these very assumptions and argues that:

- What gives the resource a basis for sustained competitive advantage is its scarcity and not ubiquity.
- Proprietary technologies may afford advantage for a while. However, infrastructure technologies afford advantages only when they are shared (telephones, roads, and so on).
- Perception of market changes is of value up to a point.

'IT has all the hall-marks of an infrastructure technology' (Carr 2003). IT is first of all a transport mechanism. It is more valuable when shared than when used in isolation.

We do appreciate the weighty arguments put forward. These signals are useful as a warning that a very critical look is necessary before a decision is taken. However, one cannot forget that underinvestment in technology could be a great peril. Further, we must also bear in mind that what technology provides are essentially tools for thought. The organization would have to decide how to use these.

In these matters, smart deployment of funds (where and when to invest) and the timing would alone ensure a sustainable and differential advantage. The FIs have to decide if they should be leaders or should they be followers who wait till the costs come down. These are thorny questions and would need to be looked at with utmost care.

Last, productivity gains come from managerial innovation. Fundamental changes in the way companies do business can come about through technology deployment along with improved processes and capabilities. These alone would account for productivity gains and innovations.

In almost every seminar and discussion group, there is generally a reference to the failure of dot com companies in the year 2000 and thereafter. The fact that the CEOs of such companies made huge profits personally while their companies became bankrupt lends a certain moral indignation to the tenor of discussion.

The failure of the dot com companies could be attributed to a number of factors. The principal one was the exaggerated claims made by them. Let us look at the case of stand-alone e-banks. It was suggested that the negligible transaction costs of these banks would force the traditional branch banking out of business and that we would have banking, but not banks and their branches. With this end in view, lavish amounts were spent on advertising and the basic rudiments of commercial banking were thrown to the wind. The rates charged to the borrowers were less than the ones paid to their deposit customers. The reduced costs could not compensate for such losses. The result was foregone.

There is another aspect and that is perhaps more significant. Obviously organizations with an established customer base and a network of branches could not let go the advantages so easily. They developed their own e-finance channels and what came to be known as a brick-click operation came into vogue and found great acceptance with the customers.

Further, many organizations experienced intense customer pressure for building such channels and were willy-nilly driven to it. They were forced to ignore its viability.

14 E-finance

There is another angle to this development. The idea that a dot com venture meant high hopes and aspirations, but no substantial business plan or model, is a lie. A number of established companies have now developed these channels and are using them very successfully. It must also be mentioned that a number of stand-alone banks have also weathered the earlier difficult times and come out quite successfully after a given time.

This chapter, albeit briefly, shows that the failure of these early ventures has not put a stop to these activities, but, increasingly, they are being successfully used by financial services industry and other commercial enterprises.

At this stage it is important to turn our attention to the technology aspects.

HOW PERVASIVE WOULD THE INTERNET BE?

Is it a mere sectoral application or would it affect every aspect of our life? The issues are no doubt controversial. Recent articles in the *Harvard Business Review* seem to suggest that the developments are not universally encompassing, but have only a limited application. We, however, are prone to agree with the views expressed at the Berkley Roundtable (Cohen et al. 2000). A summarized version of the views propounded there is given here. Allen Greenspan, Chairman, Federal Reserve, sees in the present development(s) 'a deep seated (and) still developing shift in our economic landscape' caused by 'an unexpected leap in technology'. The new emerging economy is variously described as 'innovative economy', 'knowledge economy' or 'a new weightless economy'. We ourselves would use the terminology made familiar by the Berkley Roundtable and would term it as 'e-economy'. The e-economy is a structural shift, bringing transformations and disruption. Today we are in an era where the whole economy and the social structure resting on it are undergoing a change. The driving force is information technology.

IT amplifies brainpower in ways analogous to ways in which the 19th century Industrial Revolution's technology of steam engines, metallurgy and giant power tools multiplied muscle power. IT builds tools to manipulate, organize, transmit and store information in digital form. Far more important is the way it changes the way we think.

IT builds the most all-purpose tools for thought. The capabilities created to process and distribute digital data multiply the scale and speed with which thought and information can be applied. The connectivity and computing

power have resulted in 'e-economy' emerging faster and is more widely diffused than the previous revolutions.

However, we must admit that at this point it is difficult to estimate the full magnitude of changes set in motion. It is like aiming at a bird, which is not only indistinct, but also moving at a very high speed in a zigzag fashion. One thing is certain, it is widely pervasive and would continue to pervade more and more eco-activities.

The next section analyses the effect of the upgraded technology in the way it would affect costs.

Sources of Cost Savings

The internet has the potential to increase productivity growth in a variety distinct ways:

- The costs of many transactions could be reduced. The distribution costs could be substantially brought down.
- The supply chain management could be managed far more efficiently.
- The broadening of markets could lead to a certain pressure on suppliers to use techniques, which could reduce savings.

Electronic processing of claims by the insurers could bring down the cost of claim processing from US\$10–15 to a few cents. Same is the case on presentment of bills and payments thereof. The internet could help in better scheduling and information sharing across the company, more efficient interaction with other firms and elimination of some intermediaries altogether.

Enhanced Competition Translated into Cost Savings

It is likely that the degree of competition could make the whole economic system more competitive by bringing many markets closer and provision of information could lead to more efficient production and greater consumer satisfaction. We are led to believe that the internet would lead to enhanced productivity growth over the years. Great impact would also be felt in a wide range of 'old economy' sectors. There would be considerable improvement in business performance by encouraging competition. Across the financial

16 E-finance

services industry, retail banking is a major source of difficulties in making the transition to internet operations. Financial services based on provision of services to customers through relationships tied to geography and the provider's knowledge of the customer will necessarily have to weigh the advantages and examine if any savings were achieved through migration by the customers on the internet for standard financial products. The impact is very clearly evident in brokerage services, where the internet has not only reduced the costs, but has also strengthened the relationship-dependent services of investment advising and portfolio management in addition to the standardized service of stock trading. Customers benefit from cheaper trading on-line and have the added advantage of the research findings, analysis, and so on, from the brokers. We must, however, add that some of the cost reduction is offset by increased advertising and marketing costs as online brokers compete with one other.

The internet allows effective asynchronous communication so that information access can take place any time the investor desires. It could well be in the middle of the night. Internet allows flexibility in dealing with information and in an interactive manner. The search capability is enormous. It is far superior to catalogues/menu-driven telephone conversations.

In the current uncertainty prevailing in the financial sector, the Indian financial service providers will have to improve their work methods and culture so that customers overseas (not merely non-resident Indians) are attracted to the Indian markets. This aspect would need careful review as this would set in motion both marketing and technology developments which would lead to improvements in the working systems. The thrust area would be job enrichment, bringing in a new work culture and developing the skills of the staff members to transform them to knowledge workers.

Websites

During the last few years the financial services industry in India has taken giant strides in making internet facilities available to their clients. A major part in attracting clients is played by the websites which are the entry points. Generally speaking, after the introduction of websites there is a tendency to wait and hope for the customers to start using it. It is looked on as a permanent fixture. This approach has to undergo a radical change. The websites should be looked at as gateways to induce the new customers to avail of banks' services. This line of approach is being advocated as a number of financial institutions including even the Islamic banks have made claims about the soundness of their systems.

This chapter looks at the development of websites and discusses some interesting legal aspects pertaining to cyber laws. Indian banks could well try and secure some business from overseas customers not only by propagating a business model similar to the one provided by their erstwhile bankers/financial service providers, but also by providing a policy frame which can help in weathering the storm of present financial crisis without much difficulty. There are some European cases which would make one realize the importance which needs to be attached to this aspect of the problem.

Having decided to offer internet services, the organization must take steps to ensure that all that was promised is duly delivered. The task for each one of the staff member is to discover how to do the job in a better way. In the network economy where machines do the jobs, the task for each worker is not how to do the job right, but to ascertain the right job to do. One should be looking for opportunities. It needs to be reiterated that unless an organization has critically evaluated all these factors it would be quite harmful to the organization's interest in the long run.

18 E-finance

Before proceeding further a word of caution is necessary. It is customary to herald one's entry or even a proposed entry by saying that the organization would offer anytime-anywhere banking and other services. It may be a good advertisement, but it should not be the sole aim for an organization about to launch its activities. TV advertisements can be misleading. These advertisements often conjure pictures of yuppies talking to their US brokers from Trafalgar Square and disturbing the pigeons by their joyous shouts! One could, as a Nomura executive told the author, access their New York/Tokyo offices even from the middle of Sahara Desert. True it is. But one has to be equally concerned with bread and butter activities and their implementation. A lot of misconceptions prevail and it is necessary to look at the elements of the process.

The current phase of developments indicates that the way ahead would be for established organizations (banks, brokerage houses, and so on, with branch network) to offer these services. It could be pointed out that some stand-alone banks have weathered the storms and are now firmly entrenched. The generally prevalent pattern is what is now called the 'Brick and Click model'. Predominant e-finance business models involve multi channel distribution. Most of the online vendors are entrenched financial conglomerates that use the internet as a channel for marketing and distributing their financial products.

Most of the competition for online client acquisition focuses on the layout functionality and facilities offered by a financial institute's web presence. From a client's perspective one could divide the online interface into five categories:

- Company specific websites.
- Directories and information portals.
- Vertical integrators.
- Point of sale sites: product marketing through various themes based web-pager.
- Value added portals: websites empowering consumers beyond mere listing and linking.
- Aggregator portals: price and quality comparison across a number of services of providers.

Perhaps a frequently used classification of services offered is by having recourse to delivery channels.

Access Devices

These devices include personal computers, personal digital assistants, televisions equipped with internet access or cellular phones and other wireless communication devices. Portals could supplement these.

Portals

Portals are becoming the critical link between access devices and financial service companies. Portals offer access to a range of financial service providers often for free or a fixed price, but generate revenues from fees paid by providers referred through the portals. These include portals designed by specialized financial service companies as well as general portals like AOL, Yahoo, and so on. Aggregators complement portals allowing consumers to compare mortgage insurance or other lending products offered by finance companies, enabling companies to support existing financial service providers as well as specialized financial service providers, and virtual banks' specialized software.

THE ONLINE VALUE CHAIN

The online value chain is a useful way to think of the important roles that will exist in delivery of online services to customers. The banks/FIs are 'manufacturers' of market products and process information (content). The delivery is through a network. The customer accesses it through various devices like personal computers (PC), mobile telephones, televisions, and so on. The organization would need to take a view as to which access device would be suitable for a given activity.

Filling in a loan application would necessarily have to be a PC-based activity as using the TV for such work would be impossible. However, care has to be taken to see the users' preference in accessing through a particular device.

We will now, briefly, touch on the problems associated with some of the aspects concerning entry into e-finance. Obviously the first thing that comes to one's mind is the establishment of a website.

20 E-finance

Very often, the bank designs and builds a website, but it is not of much use. It seems that in such cases, much thought was not put into building the website. At one level, the problem to be resolved is whether we expect the access through PCs or mobile phones. Second problem relates to the information to be presented. In an article in Bank Marketing (Bachman 2001), launching of a website has been compared to dressing for an Academy Awards presentation 'function'. A financial institution must make its presence felt. After all, the web would be the vehicle for building loyalty and business.

The internet is unlike any other form of communication. Unlike a pamphlet or an advertisement, the internet is an interactive medium that is rapidly evolving. Organizations need constantly to maintain and upgrade their websites as technology and customer habits change. The list given below lays down a few areas, which would help FIs and others in designing new websites and also help those who are seeking to improve their existing set.

- Whatever be your intended audience, the website must reflect your strategic choice. It must clearly reflect what the organization is trying to achieve, for example, selling new products to existing customers; attracting new customers from other markets; or providing information to existing stockholders. These objectives should be specific and documented.
- The website is an information site and not a glitz. The site must satisfy highly directed visitors in search of specific information. It is not for entertainment.
- The graphical mode of presentation is a great advantage. Further, even video clips can be added. But it must be remembered that frequent visitors to websites get tired if they have to see the same picture or hear the same notes.
- Never create an entry page that takes longer than 15 seconds to download. Otherwise the customer would leave and not return again.
- Avoid any features that would cause the browser to crash, freeze or show error messages.
- If possible design pages to target customer segments.
- Provision of investment calculators could be a great help and should normally bring the visitors back.
- If possible add links to outside websites.
- There must be an incentive(s) to visit the site over and over again.
- Easy navigation is extremely important.
- One must never forget that every customer does not have access to a high speed, dedicated link.

It needs to be added at this stage that website experience may not augur well for interactive digital TV, PDA (Personal Digital Assistants), mobile phones, and so on. A survey conducted by Microsoft for Barclays and Nat West banks has found that the content has to be compelling in order to get the user to visit the site.

Designs for PC and TV viewing have to be different. In case of TV you are watching from a distance and in case of PC you are close by. The cell phones are a different cup of tea altogether. The differences are writ large. The small size of the screen necessitates that you offer altogether different solutions. It is now increasingly realized that FIs must not jump on to the bandwagon blindly. They must consider the limitations and issues that surround such a strategy.

However, there is an extremely cautionary advice that must be offered in concluding this section on web design and its use. If using the internet is to be successful, there has to be an operational efficiency behind it to fulfill the promises, which have been made to the clients, otherwise an institution's reputation can be at risk.

AGGREGATORS

With the help of the internet one finds that the one-stop portal is a reality. To begin with the reasons for developing such portals need to be discussed. The need to have a website where customers could handle all of their financial affairs was thought to be the prime need. But one element was missing here. The customers were unable to carry out transactions from their multiple accounts at the same time. The concept of designing a home page that might have broader utility for the user than mere transaction processing and information delivery has some merits.

At this stage, it might be useful to clearly define the terms used. 'Aggregation' refers to gathering information from multiple websites and delivering it to a customer's account at a single website. Consolidation refers to gathering information about a customer's several accounts at the same website and presenting it to the consumer as an integrated statement.

Various types of portals (an outbound website gateway that links to other sites and an inbound gateway that presents information gathered from other sites) have been created. The really useful portals are part search engine, and part tool kit, calculator and part information market place. These portals (a) are an easy way to do research about different kinds of products, (b) send and receive email, (c) provide information and stock prices and (d) are a model scenario for taking a wide range of decisions.

22 E-finance

The best example of an aggregator is the 'Lending Tree' which could best be described as a 'market place for lenders'. There is no doubt some truth in saying that these portals are useful on a pre-transaction basis rather than for an ongoing relationship.

Another type of aggregator (the account aggregator) places more emphasis on ongoing relationship building. These portals offer information, but very little by way of assessment. Many FIs are, therefore, providing tools to do so. These tools can and do help customers to have a better asset allocation. There is also a tendency to have links with associated activities like broking.

At a seminar on e-banking we found that many of the participants had apprehensions about the technology to be used for introducing such features. However, some of the speakers rightly mentioned that it was not exactly rocket science. It is a distinctly low-tech application and goes by the name of 'screen scraping'. It enables an aggregator to go to any financial site and that too with the customer's prior consent (not the service provider's). The aggregator makes the server think that it is the customer's routine request. The system, of course, needs a lot of maintenance. The 'security' aspects of such transactions have been discussed in a later chapter.

There are, however, serious challenges ahead. It is being gradually realized that the internet is not a stand-alone business proposition, but must be a part of a larger delivery capability. Integrating internet channel information, customer knowledge and transaction information with those at the branch, call centre, and ATM is a critical issue. The portal concept must be thought of within the context of a larger multi-channel delivery capability. The branch or call centre must have much more detailed information so that genuinely customer centered information can be provided.

Currently, the web services ought to be used to enhance internal efforts to integrate applications together in a product or process value chain.

E-BANKING AND ONLINE TRADING

These two topics have been discussed in detail in the later chapters. Here we would touch on some common difficulties experienced at the implementation stage. A major problem relates to cost escalations. The problems could be overwhelming unless one is aware and takes care right before going in.

The main culprit here is the professional fee for consultants. It is not always necessary that the vendor engineers are the most proficient ones.

In fact, most of the vendors send only the second or third line of consultants/engineers for implementation projects. This means that while the vendor consultants are refining their skills on their product, you keep paying more and more. Or you become their training ground. Besides, the professional service effort is always an estimated effort; you can not bind the vendor once the work agreement is signed off.

In situations where the system integration has to be done between two different systems, such as in the case of internet banking or treasury systems, which have to be connected to the core banking system using Application Programming Interface (API), the risk of cost escalation on this account increases many folds. The one way out seems to be to provide for a fixed charge for professional services. Most probably you will have selected the product through a quotation process from a number of vendors. And you can insist on a fixed charge for the professional services, else the quotations have no meaning. Another alternative is to have a man-days budget with a variation cap incorporated in the contract.

The decision-making process in most of the banks is such that in spite of the budget having been approved for the project, for every decision—be it for a business requirements specifications or be it for an item of expenditure—days and sometimes weeks are lost. They have to approach the same sanctioning authority and, hence, the delay. In today's atmosphere where vigilance is a bugbear most bankers are scared of, matters are referred to the original sanctioning authority, which in these cases is the board. The way these boards are (for that matter any board functions), cost escalations are not viewed very favourably. This will throw any project plan and manpower budget out of gear. And a vendor, who has calculated and committed the price quotation on a reasonably tight budget, will incur heavy losses. Hence, if you manage to get a fixed manpower budget in the contract, please have a foolproof decision making and expenditure sanction machinery in place for the project. Built in escalations/contingency provisions ranging from 10–20 per cent are hardly the solution. The recommending department's actions in allowing such cost escalations would be viewed with suspicion. It is better to sit down with vendors and try to identify areas where there could be delays and escalations and prepare a budget for them. The background notes should highlight these.

The essence here is that unless you find a way to control the professional service charge for your project, your entire financial estimates for the project is at the risk of going for a toss. At the same time if a vendor commits you a fixed professional service charge and you do not support him with an efficient decision-making system for the project, the vendor will have

24 E-finance

no option but to abandon the project mid-way. Both the conditions have equally unpleasant consequences for you.

Rather these are unforeseen costs, some of which one would normally fail to see at the beginning when you are preparing your budget. Some of the more obvious expenditure items that are left out at the time of initial budgeting have been listed below. Individually, these appear to be small, but together they become a substantial part of the total cost. And if you miss out on these, it is going to be questioned later on.

- Hardware and Software for backup system and test system.
- Firewall System: hardware, OS and software.
- Firewall for back up system.
- Encryption mechanism.
- Web server certificates.
- Leased line and backup connection costs.
- Security policy design, validation and auditing cost.
- Disaster Recovery Center (DRC) costs.
- Risk Management and contingency plan.
- Costs of hiring/buying computers for project implementation and UAT.
- Costs involved in hiring consultant(s) for techno-legal planning.
- Process change management.
- Setting up new data centre or expanding the existing one.
- Leased line and encryption of data between data center and DRC.
- New support resources and their training.
- Telephone bills, transport and hotel charges for consultants.
- Additional costs due to people working late, working on holidays and weekends.

Some of the aspects touched on here may appear to be too obvious. Our own experience suggests that these very aspects can cause a lot more difficulties, as they were never anticipated.

OUTSOURCING VERSUS DOING IT YOURSELF

The technology arena is a harsh unforgiving environment where the expected end result is very high and mistakes or flops are considered worse than bad loans. For any bank/financial institution, wishing to implement

its own in-house system, the main consideration should be regarding the availability of people. Experienced, 10-hour-a-day workers, who are not only dedicated, but are also not risk averse is a prime necessity.

Figuring out the right cost for the project is the next task. Generalizations based on comparisons with other banks or institutions can be totally misleading. There are specific measures and techniques to determine the appropriateness of technology in a given institution. The normal thing is to compare it with the workload. In case of anticipated activities certain conjectural thumb rules have to be used.

The advantages of having work done in-house has been discussed in the following paragraphs. Two major advantages are control and costs. In today's competitive environment it is essential to have both these aspects properly taken care of. The banks/financial institutions would have dedicated support, which no outsourcing agency can match. Further the system can take care of certain overload without much extra costs. It can be said that stable systems last even for 5–7 years and since the depreciation on these items is probably complete in three/four years the system availability is for free. Customization may be possible if the banks were to approach the vendors right from the start.

Outsourcing has its advantages too. One can have ready-made expertise. Instead of hiring additional staff, the banks could follow Drucker's (2002) 'Consultant' model and make do with such specialists, as it would certainly be cost-effective. Almost 20 per cent of the costs are incurred on welfare and statutory benefits. A right outsource company may deliver products as operational solutions. Let the outside specialists do the work and let the bank use the results. Banks also can take advantage of the research work done by their vendors. The possibility of the outsource company and bank becoming partners after working closely cannot be ruled out. Staff turnover at senior levels would create substantial problems for the bank, but not for an outsourcing firm.

One can go on listing the merits and demerits of such options. The final decision would always be a result of diverse factors being balanced. One only hopes that these complex matters would be examined in depth and roadblocks identified so that the transition is smooth.

It needs to be added that staff training would be of paramount importance to achieve the desired results. There has to be considerable emphasis, during training, on security aspects as also on care to be taken while performing normal routine functions. It is also important to ensure that the participants internalize the need for as prompt a response as possible. The

26 E-finance

system designers would sooner than later have to provide facilities to the concerned staff such that the customer queries/complaints are handled as quickly as possible. There would have to be job enrichment and an equally thorough training on aspects of 'Law and Practice'. One would have to aim at being a global entity and be ready to meet such challenges. Initially the response could be from NRIs, but to meet their growing demands is also no mean task. It is important to secure the business before it is diverted to other institutions. Gradually the customers would also feel the need for a secure financial environment. It is for the FIs to take the required initiatives and do all that would be necessary. This would have to be a bold decision.

Products and Services in India

Before delving into the products and services that are offered by various service providers it is necessary to review the thrust that propelled the forays into internet services. The initial impetus came primarily from the competition within the fraternity and from those which were outside the pale of normal service providers. To an extent the stock market categorized banks as tech-savvy or otherwise forced banks into such decisions. However, subsequent developments have not quite been in consonance with the initial response. These developments could well be regarded as somewhat sluggish.

The large (very large) organizations are very often reluctant to make radical departures from the road traversed successfully. Parts of such a large organization (and in all likelihood they are the most powerful parts) are not prepared even to contemplate developments, which appear to be risky. The fear is that the new technology could end up cannibalizing their markets and destroying their divisions. One sometimes wonders if large organizations are good at fully developing and commercializing technologies. The issues have moved from the narrowly technical domain to fundamental questions of how to organize one's markets and bring about the other required changes. The policy risks are high.

There are, however, other reasons which have to some extent retarded the developments. These could be summarized as under.

- Concerns for security have held back many customers who would otherwise have opted to avail of these services. The media coverage in such cases tends to paint a somewhat exaggerated version.

28 E-finance

- The terrible delays and hassles involved in getting redress often deter the clients from pursuing these matters. One naturally tends to use the services only when it is absolutely necessary.
- The corporate customers and other 'bulk' users find that all that the institutions are promising is not translated into action. Delay in getting the promised result (for example, clearing of high value cheques) is a very common complaint voiced by the customers.
- Add to it the infrastructure problems like power outages and one can well appreciate the reluctance of clients to be solely dependant on this channel.

The competition has led to a continuous downward pressure on margins as banks and financial institutions are vying with each other for good advances. The era of asset-led growth, forces banks/financial institutions into cut-throat competition for the small cake available. The need to shore up profits by reducing transaction costs was keenly felt. Internet services did offer a way out. The financial institutions also stood to gain because transaction costs could and did come down substantially. A cash payment at the branch would cost somewhere around Rs 18–20 while the same payment through the internet would cost a few paise. Last but not the least, banks and financial institutions must learnt that successful strategies have to be built around the customer. The World Bank rightly suggests that with data mining techniques, it would be possible for banks and others to tailor schemes for individuals and charge them accordingly.

At this stage it would be worthwhile looking at some peculiar problems associated with the internet. Initially, it was felt that stand-alone e-banking institutions would overtake brick and mortar banks and that the latter would wither away. This was more a conceptual fantasy and the 'brick/click' model has come to stay. The emergence of such a model has led to certain patterns of development. However, it is a huge challenge to get behind virtual customers, their wants and help them understand emerging desires, and to move from delivering things to aiding in the understanding of self. The institutions have three options. They can develop internet-banking capabilities that support the current product, service and channel mix. This is normally referred to as the 'traditional migrator' approach. It has the advantage of reinforcing the banks' long established brand and allowing the banks to proceed with single market personality while actually using multiple delivery channels.

The second approach described as 'Continual Evolver', would be for the banks to reinvent themselves and focus primarily on extending reach on the internet channel and deepening relationships by meeting customer

needs. This would help them in clarifying confusing offerings, streamlining disparate marketing messages and committing to an ongoing culture of change. The final approach—Clean Slate Approach—is to create a new brand disconnected from its established identity. The benefits include the ability to use a low-cost base and virtual distribution to achieve new customer acquisition and deliver broad customer choice.

It is important for companies to find ways to make their history work for them. For instance, I distinctly remember the function at our zonal office when customers having their accounts with the bank for over 75 years were felicitated. For quite some time the environment was such that the services rendered by a company helped in distinguishing it from the rest. The same strategy (customer service, reliability and trust) must be used to retain the fickle customers. In India, it is not advisable to close the branches merely because they are high-cost centres. During the time when staff is trained to take over more responsible tasks as advisors/marketers, the costs incurred will have to be subsidized by low-cost internet operations. Handling of customers is always problematic. One of the difficulties is to hunt through old records and get at the bottom of things. It is worth noting that traditional financial institutions are extremely adept at retrieving information from old records and deal with customer complaints very easily. With the help of technology it might be possible for these institutions to deal with these matters in minutes. This strength needs to be built on, particularly, for customer relationship building.

At this juncture, a very broad based review of products and services offered is important. A detailed review would be available in chapters dealing with broking, banking and insurance. At this stage we would detail the broad trends in the three segments referred to earlier and deal in some depth with topics not covered in subsequent chapters. Certain peculiar aspects of the internet economy are covered in Chapter 14. Normally one would expect an increase in price with improvements in quality. This does not necessarily happen with goods traded on the internet. Similarly there are other aspects regarding costs and their behaviour which would have a bearing on the whole range of services offered. This background has to be borne in mind to appreciate the development of products and services offered.

The term e-finance refers to the provisioning of banking online, electronic trading, delivery of financial products such as insurance, mortgages and electronic money and communication of financial information and analysis over the internet or via other public networks. Financial markets now have electronic clearing and settlement—transfer of title.

E-MONEY

Broadly speaking 'e-money' represents monetary value which is stored on electronic devices and which is acceptable as a means of payment by undertakings other than the issuers.

Various types of e-money are currently in vogue. The more frequently used are card-based. E-purse schemes seem to have, unlike the card-based schemes, reached a critical mass in some countries. It is seen that card-based schemes are used more at unmanned stations (vending machines, public telephones, and so on). The contact-less cards version has significant potential, particularly at retail outlets, stadium, and so on. In the realm of server-based 'e-money' certain types like prefunded personalized online payment schemes (Pay Pal) provide these services to customers of its parent company ebay. Prepaid debit cards, electronic travellers' cheques along with other hybrid products are also available. The hybrid products are available in both prepaid and postpaid categories.

It is difficult to ascertain the amount of such money in circulation. Estimates for Europe suggest that currently it could be of the order of 450 million euros.

The convenience and security of cash payments could be available in such forms also, provided the legal certainty of acceptance is assured and the stability of issuers is ensured. The guarantee could come through capital adequacy and regulatory constraints. Of course, technological innovations must not be hampered in the process.

Mobile devices are now being widely used in countries like Japan and Korea, for internet access and use in e-money. It is the merger of internet access and traditional finance that has made such inroads possible. It is expected that in India also this transition could be made and that it would soon replace cards. The mobile recharging charges are now reduced and soon mobile companies may start offering these services and enter the payments market.

It is necessary to point out that what at one time seemed outlandish is now very much a reality. Conversion of virtual world gaming currency is now going to be made in real world currencies. Online game Entropia Universe has been granted a licence to be a bank. Issued by the Swedish Financial Supervisory Authority, the licence means the game can be more closely tied to the real-world finances of players. Mindark, the developers of the game, said that they aimed to launch a fully-functioning in-game bank within the next 12 months. At current exchange rates, 10 PED (Project Entropia Dollars) are worth one US dollar. Unlike many other

online games, which charge a monthly subscription fee, the software for Project Entropia is free to download and install. However, players pay real money to get at in-game items, such as guns, armour and other gear, and the micro-payment system pays for Entropia's running costs. The license will make it easier for players to convert real world cash into PEDs and sustain their characters in the game, said Mindark in a statement. 'We will be in a position to offer real bank services to the inhabitants of our virtual universe,' said Jan Welter Timkrans, boss of Mindark. It plans to offer players interest-bearing accounts, let them deposit their salaries and pay bills or lend cash via the in-game bank. The license also means that each account is backed by deposit insurance to the value of US\$60,000 (£42,000). Regulators will get oversight of financial transactions carried out in the game world, so they can spot if criminals are using it to launder money. Mindark claims that more than 800,000 people have registered to play the game and 80–100,000 are regular players. About US\$420m of player-to-player transactions were carried out during 2008, according to Mindark figures.

Could the mobile phones replace the PC in such transactions? It is doubtful because most of us are used to wide screens and many financial decisions need a lot more information than what a small screen can hold/display. However, we envisage a possibility of it being put to use in different ways. One could book a table at a restaurant, place an order and walk in after sometime. Basically, if delivery is innovative, getting a large number of clients on the mobile bandwagon may not be difficult. One must emphasize that wireless devices are now a part, an essential part would be the right way of saying it, of our lives. Third generation phones would make internet access easy and SMS could well become the foundation carrier. Financial institutions could ignore these aspects at their own peril.

The major users of the internet are the corporate customers. Companies increasingly use the internet based systems to cover the entire range of financial needs from managing bank accounts and bill payments to asset management and even to insurance products.

In the Business-to-Consumer (B2C) segment, the services offered include balance confirmation, transfer of balances from one account to another. Bill payment services are becoming increasingly common. ICICI bank now allows customers to pay municipal taxes on the internet. It is pertinent to note that in other countries, the competition from non-financial institutions such as Yahoo or Microsoft is quite aggressive and it is possible to witness similar developments here.

The area of 'credit' has seen some rapid developments. In many cases, application processing is available online, but complete fulfillment is not.

32 E-finance

Small- and medium-sized industries can draw trade credits and other sources of verifiable finance. Housing finance is one area where functions ranging from loan application appraising, valuation of houses to completion of loan documents are all done over the internet. The internet also provides information on financing and other options to a wide spectrum of potential house owners. It is necessary to refer to two mortgage finance providers. Advantage mortgage began as a mortgage broker. Over a period, it has become an overall aggregator like the lending tree. Fifteen leading lenders are the major source from whom it derives revenue. Advantage solicits borrowers, evaluates mortgage loan packages for presentation to borrowers, prepares all the documentation required for the loan and sends the complete loan package to the lenders. The borrowers do not pay any fee because lenders pay them.

FACTORING AND LEASING

E-finance helps in lowering the costs and increases the availability and ease of transferring the information. The ease of delivery and substantial reduction of costs are factors responsible for the widespread use in this paper intense activity. This development has increased the lender and client opportunities for factoring, which is the sale of accounts receivables and leasing which are loans collateralized by assets. Electronic transmission allows real-time information exchange between parties, increased security, immediate credit decisions and lower transaction costs.

A development (in India itself) which has not attracted much attention is the development of internet platforms to trade and pledge electronic warehouse receipts. This may reduce the need for government to purchase commodities for stock piling. Letters of credit, bills of lading and other documents associated with trade funds are also gradually being taken over under the e-finance umbrella. Bolero.net is a joint society for Worldwide Interbank Financial Telecommunications amongst commercial banks, freight forwarders and shippers. It could certainly help in automating trade finance process.

Credit Disbursement for the Weaker Segment

It is often asked if the internet would be useful in the area of micro finance. Two cases merit a discussion. South Africa's Standard Bank has bundled

services required by the poor and it is a viable activity for the bank. The second case is that of Grameen Bank in Bangladesh. The bank sells pay phones to borrowers of Grameen Bank and these are made available to all the villagers. A number of women have turned cow-rearing or grocery activities into profitable ventures. Action International is using handheld computers to cut costs and time to sanction loans. Entering the data takes about 25 minutes and processing takes about one hour. The new micro loan-processing software designed for palm-pilots, allows loan officers to record client data, take applications and make loans on the spot. Pla Net Finance is the first international organization to refinance micro-finance institutions. In fact, Pla Net hopes to help micro finance institutions through all stages of their development.

E-TRADING IN SECURITIES, EQUITIES AND FOREIGN EXCHANGE

Electronic Trading Systems provide some or all of the following services: electronic order routing, automated trade execution and post-trade information. Online trading systems can be divided into various categories according to:

- Trade model used.
- The ownership structure of the system.
- Sources of prices for securities.
- Customers.
- Coverage.

E-TRADING IN EQUITY MARKETS

The trading models in equity markets can be divided into two categories. Order-driven systems combine all bids, ask orders into one central order book and automatically match the orders without intermediaries. The other is the direct access trading. The investor makes an order online, the brokerage firm routes the order directly to a market maker and gets a commission from the market maker for what is known as 'payment for order flows'.

E-PROCUREMENT

It is an off shoot of falling margins. The financial institutions focused on e-procurement for corporate supplies. They could leverage their role as payment facilitators. The entire process of purchases was streamlined and savings affected. ABN Amro, Bank of America, Citi and Chase Manhattan are some of the leading participants in the process.

It is important to present a road map which Indian banks/financial institutions may like to follow. Increasingly the corporate clients (particularly those rated highly by rating agencies) are no longer dependent on banks for their credit requirements. The issuance of commercial paper, suppliers' credit and recourse to global capital markets have led to banks and financial institutions pursuing (chasing) the corporate clients for a slice of assets. It is, therefore, not surprising that most banks are focusing their attention on small- and medium-sized enterprises. State Bank of India and ICICI bank have all set aside hefty sums for this sector.

The whole procedure right from origination of application to sanction and loan disbursement is extremely dilatory. This is where internet could be harnessed to speed up the process. Credit rating and or scoring tools are available with many banks and these are used at the time of considering consumer loan applications. The same could be extended to small- and medium-sized sector and delays avoided. Further, many of such units use computer-based accounting packages and banks could offer advice to the customers in areas like receivable management, cash management, and so on. This is however a novel proposal. It envisages building a 'virtual' market for their products. All the banks together can provide a market place for their small and medium clients by acting as a clearinghouse for products manufactured by their clients. A similar exercise was undertaken for a bank at the state level and the bank brought out a directory of products manufactured by the bank's clients and it turned out to be extremely useful.

Currently, a survey is being undertaken by us with the help of a bank to ascertain the requirements of small and medium clients and it is likely to lead to the introduction of internet facilities by the bank concerned. Purely from a lender's point of view, it would afford a degree of control never before thought possible or feasible. It would assist the industry and the banks in building a unique partnership and in creating a healthy appreciation of each other's problems.

Another segment which is somewhat neglected is that of senior citizens. Banks and particularly cooperative banks, could conduct classes for senior

citizens and induce them to use the internet facilities. For them it is a prime necessity. Mobile telephones could meet their requirements. Cash withdrawals and deposits may not be possible. But a courier service, run by the bank and other income-generating services, could be provided while meeting a great social need.

In countries as diverse as the Republic of Korea, Mexico and Philippines, insurance products are being increasingly offered to clients both electronically and through intermediaries. In India, Insurance Regulatory and Development Authority (IRDA) has not yet accorded its approval to issuance of policies on the internet as the digital signature certification mechanism is not fully in place and not easily accessible. There is also a certain degree of reluctance on the part of customers to buy insurance on the internet.

However, it is increasingly clear that financial services firms have now to hasten the pace of change. They must realize that they do not have much waiting time and would encounter a number of threats to existing competitive positions. The need of the hour is 'information freedom'. It is about transforming island processes into extended ones. It is about integrating the complete chain of events that information available anywhere must be made available across the entire network. Organizations must learn to take advantage of information available with them. With a bit of slogan mongering one could assert 'integrate or die'.

Discussion with some overseas bankers, who had been offering such services for some time, brought out the following general observations in respect of product development.

- The old axiom 'build it and they will come' is a model that does not work online.
- A full range of products, including brokerage and financial planning tools, a trusted brand name, a multifunctional but easy to navigate website and responsive customer service, is a must.
- There is a constant need for adding functionality and new products. Customers should be able to do more things online than they do at a branch.
- There is an acute need to unbundle financial products so that a person who does not want face-to-face relationship can get whatever help/advice he requires.
- Bad service really ticks off online customers. Customer service is an offensive weapon in the marketing artillery of any web-based company.

36 E-finance

In conclusion, it could be said that to gauge the future we would have to think 'both/and'. The future is digital. It is also analog. Those who talk of paperless office should remember that paper is an amazingly efficient and a cost-effective display medium. The wrong question is how to get rid of paper. The right question is what should be on paper versus a digital document.

Organizations have also to make other changes and these relate to job enrichment of staff and reassessing the role of branches in the new setup. Many of the routine functions are taken over by machines and there is an acute need to reorient the work systems at the branch level. The branch would necessarily have to be a profit centre for such diverse channels and must be responsible for marketing and advisory services. Clients do need guidance in managing their wealth and do look up to the bank staff to assist them. In these uncertain times the staff could play a crucial role in building the required confidence levels. Closing down the branches could be easily done. But making them an integral part of the new environmental responses would require foresight and planned efforts.

E-banking and E-insurance

For the sake of analytical convenience, this chapter has been divided into three sections. Section 1 deals with problems and policy framework for small- and medium-sized banks which are entering the field of e-banking and e-insurance for the first time. Section 2 deals with the experience of the banks, which have internet facilities available for their customers and analyses the impact of this additional channel. The last section examines possibilities of stand-alone e-banks entering the field and the penetration of mobile banking.

To begin with a definition of e-banking is important as various authorities/users have different perceptions about the definition of e-banking. E-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic and interactive communication channels. E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the internet. Customers access e-banking services using an intelligent electronic device such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), kiosk or touch tone telephone. We would be using this definition in the text. However, it might be useful to quote the OECD version too. 'An electronic finance transaction is a financial transaction that depends on the internet or a similar network to which households or non-financial enterprises have access. The trade in electronic finance is the part of an electronic finance transaction that relates to the exchange of remunerated financial services' (Christiansen 2001). Importantly, this implies an element of service provisioning for it to constitute a trade in e-finance service.

About five years back there was considerable uncertainty if banks would go in for e-banking. The *Asian Banking Journal* (2000), on financial institutions' preparedness to meet new challenges, showed a marked apathy on the part of bankers and others about the new channel.

We asked analysts and harassed half a dozen bankers Whom they would consider a veritable 24-carat E-Banking savvy CEO? We were referring to a CEO who could articulate an integrated electronic banking strategy, has taken decisions in that direction, and demonstrated an ability to lead his or her bank into E-Banking. We could not even get five names And the responses sometimes slow and deliberate, sometimes drawing a complete blank was telling of how few CEOs are ready to lead their organizations into the E-Banking arena.

However, the picture is now totally changed. The question, which bankers pose, is not whether, but when and how. Most of the large-sized banks do have internet facilities for their customers as against two to three banks, which started having a range of limited offerings just five years back. The number of small- and medium-sized banks wanting to go in for internet-banking facilities for their customers is also on the increase. The reasons for this change in approach are not far to seek. Most banks are apprehensive that they might not be able to access the new IT savvy customers and others who have/had heightened service standard expectations, but who have shown a marked reluctance to visit bank branches for transacting routine banking business.

The fact that banks in other parts of the world are going through a difficult patch opens up vistas for Indian financial institutions as never before. Compared to Islamic banking, the Indian system of banking has an added advantage as we follow the business model which European, American and UK banks follow. However, Indian banks have not suffered the ill effects of Western banking on account of speculative trading or total neglect of risk management practices. We have a stable system and it is by any stretch of imagination a fairly sound and safe one. One would have to be good at connecting the dots and see the big picture.

It would be interesting to see the kind of customers targeted by banks or the general profile that banks have for their 'potential' customers. They are in the age group of 25–35, tech savvy, have sufficiently diverse needs for financial services and need to be handled with care, as the other bank is just a click away. It is natural that banks should be in a hurry to go in for the latest technology available and make delivery channels available to attract new customers.

SECTION 1

This section analyses the problems encountered by small- and medium-sized banks making their forays into internet banking. These small- and medium-sized banks need to analyse their preparedness for such changes before being lured by high-pressure technology sales people into going in for updates, which could, in the long run, not give the desired results. It is true that banks both large- and medium-sized have other problems, which could, to some extent, hinder their progress, but technology could be of some help in solving them. Perhaps, these could be mitigated by adoption of the new technology. Some of these are briefly referred to in the following section.

- Large work force: They are used to job security, are not exposed to working in a competitive environment and are somewhat reluctant to upgrade the skills required to work in an automated environment. The clamp down on recruitment has resulted in the workforce comprising middle-aged staff with 15–20 years of service behind them. This, therefore, leads to high transaction costs.
- Slow pace of ‘technology change’.
- Indifference towards customer service.
- ‘Thinning’ margins.
- Falling share in foreign exchange business.
- Competition from hostile ambience of retail markets.
- A rather inefficient treasury function.

It is understood that banks, which lag behind in the technology up-gradation process are likely to suffer over a period of time. However, it does not mean that banks need to rush in and decide on these issues. Experience suggests that the banks need to pay considerable attention to the planning phase. In this content a discussion by the Federal Deposit Insurance Corporation (FDIC) on electronic banking examination is important. The main elements that need to be kept in sight at the planning stage have been discussed here to some extent and would be mentioned again in Chapter 13.

Planning and Development

- Inadequate decision processes while considering, planning and implementing electronic capabilities.

40 E-finance

- Impact of technology costs and pricing decisions.
- Strategic implications of activities.
- System design and capability and its compatibility with customer demands.
- Uncertain applicability of insurance coverage of electronic activities.

Equally significant are technical competencies, the bank's control procedures, confidentiality of information, and so on.

The Planning Phase

The banks would need a clear view of both their brand positioning and what type of organization they want to be. They must, if they have not done so, undertake step-by-step planning to:

- Identify their priorities and determine critical success factors.
- Create an e-business road map. The bank must be able to deliver solutions quickly without sacrificing long-term flexibility.
- Every phase of the planning process should focus on delivering solutions that meet and exceed customer expectations.
- Decide on the resources required, both in terms of costs and in terms of people to successfully deliver e-programmes. Technology and business strategy (as is being repeatedly stressed by us) must go hand in hand. 'E-channel' must be consistent with the overall direction of e-business.

Before taking up specific issues, it might be useful to remember that for established banks the problem is wringing optimal performance from traditional business lines while simultaneously transforming their banks as competitors in e-commerce. A major financial upheaval would and does put a restraint on resources available for reinvestment in commerce and reignite concerns about stability of earnings. However, the fact is that the geography-centred banking model is being supplanted by an electronic system.

The experience of stand-alone banks and in some cases their failure has led to an integrated banking structure known as 'Brick & Click' and is becoming an industry 'norm'. An equally important reason for the emergence of such an integrated structure is due to the response of the existing banks to the emergence of these new entities. According to *The Economist* (2001) 'Their physical rivals have become wiser, launching their own

integrated strategies (clicks and bricks) that offer customers electronic access as well as dark satanic branches' (*The Economist* 2001). They allow their customers to do their banking online. Further, the customers also were not too keen to throw away the 'yoke' of branches. Customers, on the other hand, seem to fret about the security of e-banking. Traditional banks are thought to be more secure. It was also shown earlier that while marginal costs may be negligible, fixed costs are substantial for stand-alone banks.

How should the banks then approach the problem(s)? The banks intending to solve the problem must realize that they cannot look on internet banking as part apart. It is not difficult to list out the dos and don'ts. However, a more convincing evidence can be provided by citing three specific country experiences. Following are some of the priorities IT departments should keep in mind.

- The architectural vision to avoid costly short-term investment decisions.
- Evolution of systems as opposed to 'revolution' as one Assistant General manager in charge of IT called it.
- Careful selection of language to have an easy interface (say XML).
- Choosing the right middleware system.

All of us have been witness to the early efforts towards computerization. The deadlines, the number of branches to be computerized, and so on, had to be taken into account to achieve certain ends. The fact that few IT departments would have the breathing time to look at the future could be a worrying fact. They would be under intense pressure to bolt it to the existing system. A word of caution is in place. The latest may not be the best route to operational efficiency. The important question is how these fit into the mid-to-long-term view of the IT infrastructure of the bank.

The banks that have decided to explore the e-banking route are, in the first instance, likely to use the Application Service Providers (ASPs). The reason for this is that the policies pursued by HDFC bank, in India, which is looked on not only as 'technically savvy', but also highly profitable and, therefore, a model worth emulating. Its treasury, corporate and even retail activities are mostly automated with a strong focus on online connectivity and e-commerce. They use (in partnership with I-Flex solutions) e-commerce solutions provided by I-Flex. Wipro handles their data centre management. HDFC is now able to provide Application Support Services to other banks. Realizing that there is a huge niche market awaiting developments, ASPs would be able to play a useful role.

In fact, the ASPs, worldwide, are a growing tribe. The problem is to choose one, which would meet the banks' needs properly and then give it a try. There are, no doubt, certain advantages in going the ASP route. A bank could achieve its automation objectives without huge capital investments and with least costs. The HDFC bank and I-flex have formed a business partnership to provide such services to small- and medium-sized banks. This would facilitate use of such services by small banks.

Choosing the ASP

How can a bank decide which ASP to choose? Gartner has pointed out that an ASP should have a strong focus in the industry, a good brand name and develop real know-how with specific tailored solutions. Although these characteristics would make the ASP quite acceptable, it must also provide some unique, specific software solutions, which would ensure a competitive edge for the bank. Banks' automation, so far, has been one of a standardized 'one-size fit all' solutions. In order to do this four to five software vendors were identified and banks were asked to choose from amongst those. It is almost forgotten that automation could be a major competitive tool. It is also not certain whether the outsourcing environment is adequately and truly secured by confidentiality conditions. There is a genuine concern regarding this because the ASPs would then not be able to assess specific customer requirements or problems faced by the bank(s). They would offer only general solutions.

In this context, it could be said that the transformation to e-banking does necessitate considerable preparations within the bank itself. Training of staff is a major problem. Professor Padwal has attempted an estimate of the quantitative dimensions of the training problem and they look forbidding (see Padwal 2000). Further, it is possible that not every bank customer has access to a high-speed dedicated line(s). Many people might have a slow internet connection (56k modem connection) and might have to wait for 10–15 minutes just to know the balance. This is not a worthwhile activity.

Many banks had taken the first step in this area by building their own websites. We begin with a review of these.

Bank Websites

The problems faced by banks in building and maintaining their websites have been touched upon previously. Today, online delivery is not only

about websites accessed through PCs. Banks' customers would soon look to a plethora of online devices like PDAs (Personal Digital Assistants) and mobile phones (WAP enabled). Once again, the spread of mobile phones would make it essential for those banks, which already have their websites, to rethink about the design on the lines previously indicated in chapter on web designing.

When a bank embarks on a technology solution, it is essential that it does not blindly jump on the bandwagon, but critically looks at the limitations and issues that surround such a strategy. Further, the bank must never lose customer focus, as solutions are for the benefits of the customer also. Accepting multi-channel delivery in e-world is a necessity. To a great extent, the design for services for these channels depends on human behaviour and the financial institutions that recognize this and understand how best to present the services to their customers would be the most successful.

There is one major pitfall that should be avoided. Although anywhere—anytime banking would imply that the bank is ready to offer all services across all devices, it is a totally useless concept which ignores not only the functionality of a channel but also people behaviour. Banks must have prior knowledge about the way a consumer looks at a product and the way he/she is likely to approach the bank.

Around the time when the ATMs were making inroads in the banking sector, the chairman of Barclays bank told us in a discussion that ATMs ignore the possibility of a customer wanting to talk to the bank. There is actually a thing as a human touch. His advice then was not to underestimate this aspect, and this is valid even today. Further, correctly looked at and handled, banks could ill-afford to ignore this opportunity for a feedback session!

Will relationships between a small customer and business go the way of horse and buggy? Will bank products be primarily sold in the financial market place as commodities or will personal service and contact still matter?

Attacks on Banks' Websites

At this stage, it has to be highlighted that bank websites have been under constant attacks from hackers. Web designing must be very carefully undertaken. Further, it will be shown, in the chapter on legal issues, that the case law could be quite baffling and may lead to most unexpected judgements.

The smaller banks would naturally like to know if these efforts are rewarded. Would small banks ever see their bottom-line improving through these efforts? The survey done by the Office of the Comptroller of Currency can provide some valuable insights. How effective are internet offerings by smaller banks? And what impact do the offerings have on their profitability? The news is certainly encouraging. Institutions offering internet banking outperformed non-internet banks in terms of profitability. The Return On Equity (ROE) and accounting efficiency (non-interest expenses to net operating revenue) were higher for institutions offering internet banking than those that did not.

Before dealing with these questions in general terms, we would like to quote from the experience of two case studies based on the experience of regional banks in the US and then offer suggestions of a general nature. The case refers to Gray Bank, Georgia. The total population is about 26,000. It wants to retain its identity as an independent community bank. It now faces competition from two banks, which have moved to the locality, and also from non-bank companies offering retirement and pension products.

The bank used the internet to advertise and succeeded in signing merchant establishments in establishing an internet shopping service. The internet has been a great source for advertising the e-banking services. Apart from processing new accounts, consumer loan applications, regulatory compliances, the bank offers account opening service online, 24 hours a day. In four years it could line up 3,000 e-banking customers.

A noteworthy feature is its understanding of quality in the e-banking service competition. The e-banking service has helped in freeing up personnel to attend to other duties and more emerging services that require face-to-face attention.

This somewhat old case has been deliberately quoted to amply clarify the doubts often plaguing the minds of decision makers in smaller banks.

Some additional factors have been discussed in the following paragraphs that would help in impacting the decision. Regional rural banks/medium-sized cooperative banks should consider using profitability and demographic information to prevent usage which would be uneconomic for the banks. Customers who use internet banking and more so if they are early adopters of the internet are more profitable for the bank. Further, they are more likely to stay with the bank. 'Good Customer', profitability information, good channel usage and internal bank data on costs can prove to be extremely useful for relationship management.

- Highly profitable customers should be convinced to use internet facilities.
- Heavy users of other channels can be encouraged to shift to e-banking.
- Unprofitable customers should be avoided altogether.
- Banks should target the small personal/business relationship.

The smaller banks can build business-specific solutions and develop other kinds of systems to offer more functionality to their customers. Security policies that can be adopted by smaller banks to build trust are as follows:

- Limiting/eliminating use of email.
- Never soliciting information via email.
- Building up preauthorization processes for money transfer.
- Close monitoring of customers' bill collection requests.
- Regular contacts with customers and informing them about these efforts.

These measures would go a long way in improving the bank's image as a responsible entity in maintaining privacy and security.

SECTION 2

While reviewing the performance of large-sized banks as providers of internet services, it would be useful to briefly touch on some theoretical issues and then undertake an impact assessment. In India, barely a couple of years have passed since these services were made available to the customers and a thorough impact assessment would be possible only after some more time has elapsed. But at the same time there are some glaring weaknesses and these need to be highlighted.

The first thing any observer notices about the internet facilities is that many banks would soon (particularly, after RBI gives the go-ahead) offer many independent communication channels (mobile banking), but there does not seem to be any attempt at integrating these channels and allowing the customers to choose the channel of their preference. It is true that by increasing the number of channels financial institutions can satisfy a widely diverse clientele, but the shift away from integration of channels

could be a risky strategy in an environment where consumers demand an easy access service with an option to choose how they communicate with their banks.

The objectives, which banks have before them when they decide to go in for adding these delivery channels, will now be reviewed.

- The banks have to meet the competitive challenges and offer services at par with those offered by the competitors.
- The perceptions in the market about a bank being technically savvy also impact its share prices and indirectly affect its access to the market for capital.
- The transaction costs are going up very steeply. The costs of operations on the internet are negligible.
- The customers demand such services and the thrust is too strong to be ignored.
- Pressure on interest earnings and margins make it necessary to seek other avenues to augment the exchange and commission income.
- Possibilities of multilateral communications between branches, head offices and customers.

Although many other reasons can be provided, few banks have articulated their objectives with any degree of precision. Perhaps, this could explain the difficulties in having statistical information about even elementary aspects like utilization of services, retention of customers, income flows and plans for future expansion in cross border financing.

More surprising is the fact that specific profit centers responsible for developing the internet activities do not exist. Further, banks do not seem to have achieved a thorough integration of IT plans with the overall banking plans. It needs to be reiterated that banks should not look on internet banking as part apart.

Products Offered

For the sake of analytical convenience, products that are offered on the internet by large-sized banks will be reviewed by looking at the services offered to different segments. The broad classification between business and retail is useful to some extent, but a more detailed segment wise analysis is perhaps more helpful. It used to be customary to divide the products/services offered into two broad types—Basic and Premium products. These could be described as follows:

Basic

- Balance inquiries.
- Funds transfer.
- Bills payment.

Premium

- Includes all the basic services.
- New account setup.
- Cash management.
- Fiduciary.
- Bills presentment.
- Insurance.

A more detailed review would, in all probability, cover most of the functions as mentioned in the following list.

- Account balances/transaction histories—batch.
- Account balances/transaction histories real time.
- Account reconciliation.
- Lending.
- Account transfer—intra bank.
- Application for loans.
- Online statements.
- Transfer from deposit account to loan account.
- Electronic payments authorization schedule viewing facility.
- Electronic bill payments.
- Home loans/car loans.
- Online applications for credit cards.
- Multiple payments from a single page.
- Multiple payments on ‘us’ capability.
- Recurring multiple payments.
- Bill presentment and e-alerts.

The extent and use of these products and services cannot be exactly gauged as most banks do not keep a record of such usage. Some banks, perhaps, have attempted an exercise to determine if the workload at the branches has been reduced. The broad conclusion seems to be that the bank has succeeded in converting 80 per cent of their customers to using the internet for their transactions.

B2B Applications

Many banks are widening their online offerings by providing content and services, in addition to banking transactions. The first foray comprises of developing a port network primarily for the use of employees and corporate partners. These allow the banks' customers to communicate via a port-secure net connection. The greatest advantage of this is the security. The competitive pressures and thinning margins on banks' traditional business, are forcing banks to concentrate on developing 'relationships'. Over the past decade, banks have focused on 'efficiency' to make up for the losses suffered. In the earlier phases, banks relied on consolidation, automation, downsizing and outsourcing. However, the need to develop customer equations was ever present. The automated processes have freed the dealers, managers, and so on, to build up a relationship with corporate clients and high net worth individuals.

Apart from rendering all their existing services, banks began offering a host of other services. These have been discussed in some detail.

The corporate intranet is increasingly being used as a marketing opportunity, a way to win a position as a company's 'in-house bank' and attract customers for their online services.

Some large corporations have tens of thousands of employees, who can provide a number of opportunities. These could be described as business to employee portals offering a cluster of bundled services. Wells Fargo is offering online services (in addition to an on-site branch) to employees.

However, employee accounts are not particularly 'profitable' for banks. A number of banks undertake salary payments for the clients. The experience suggests that most employees leave only the bare minimum balance and corporate customers are reluctant to pay for the services rendered. The reason banks do this is, obviously, to build a relationship. It would be cheaper than staffing a branch at a client's site. The customer base increase does not follow merely because an intranet facility is available. Employees are not likely to switch their allegiance unless there is strong evidence. Some staff unions have expressed fear over 'big brother' watching the entire gamut of operations, while others feel it would lead to the employees being tied down to the office, reducing the necessity to visit a branch!

Banks have two choices in these matters. They can build a package, make it attractive and sell it, or they can customize products to suit employee needs. Thus, a bank may even have a 'travel agency'/vacation planning service available on its portals.

Small- and Medium-enterprise Customers

Banks today are driven to widen their services net to cover small- and medium-sized enterprises. Additionally, they also have to take care of micro financing. An inhabiting factor all along has been the transaction costs. A very crude calculation would put the average service of bank employees at around 15 years. Obviously, the costs for routine services like cash payments turns out to be very high. The internet would reduce the transaction costs significantly. Equally important would be considerable reduction in time spent in scrutinizing and sanctioning loan requirements and ensuring proper usage thereafter. A major source of annoyance for these customers is submission of routine statements to the banks. Perhaps, these can be derived by the banks and workload on the customers can be considerably reduced. However, for reasons not quite clear, our surveys undertaken with the departments in the banks have not been fruitful in persuading the customers to switch over. Banks can use a certain degree of pressure to bring about the desired result.

The micro finance agencies (NGOs, Self-help Groups [SHGs]) are, however, very keen on availing these facilities. They want to cut down on their own information system costs, and also have their field staffs get access to the accounts. They, however, expect the banks to provide a conditional access depending on the hierarchical position of the particular staff member. The prime need in offering credit and savings products to these segments is innovation in managing risks and transaction costs. They have no physical assets and banks have to overcome outreach and sustainability. Overreach in this context means 'hard to reach clients'.

The most fundamental application from the bank's point of view is back office management. A suitable computerized management information system (MIS) is a prerequisite for monitoring the quality of assets and undertaking general administration tasks. The banks have to see how they can use the internet to highlight differentiating features:

- Products offered.
- Clients served.
- Environment in which it operates.
- Non-financial information needs to be recorded and tracked. Data delay can be a problem and can easily be overcome by mobile computing applications directly into MIS. This would negate the need for back office intermediary data entry at back-office. The roll out of wireless broadband infrastructure will always enable this system to be online.

- The major difficulty faced is in the area of marketing. The SM & E customers' difficulty is in marketing. It is here the banks can help them by allowing the use of its portals for marketing their wares. The banks can go a step further by facilitating payments to the suppliers. The banks can generate a fee income for the services rendered. We had published a directory of products and their suppliers, and the scheme met with resounding success even though we did not have access to the internet.
- The banks' own purchase of stationery can be done over the internet and payments can be made directly; the kind of process reengineering undertaken by automobile companies a few years back would go a long way in helping the banks in these areas.

Assessing the Impact

Some of the difficulties in assessing the impact have been indicated, although it has only been a few years since the banks have started offering the services and it is too early to assess the impact. However, there are areas like costs to income ratios, which could throw some light on these aspects. Unfortunately, the period under review also saw considerable downsizing through voluntary retirement schemes. The impact of shifts in work technology on the bottom line cannot be isolated and whether banks are able to correctly assess their returns on technology investments is also not certain. Merely having a given channel for distribution of services is unlikely to afford any additional advantages.

A rough model to look at internet developments was used by us during seminar discussions on these aspects of the problem. It is certain that there is a distinct power shift to the customers and, therefore, it is necessary to see that the organizations make every effort to lead the pack. Currently, there are three distinct phases of development.

- Phase 1: The consumers at this stage are persuaded to use the internet and access it for their information needs at least. This phase could be used to persuade customers to migrate to the internet and also to reduce costs. It would also help in extending market reach.
- Phase 2: One notices changes in the way retail financial services are made available. There is a disaggregation. One finds that advisory services are separated from execution of services.
- Phase 3: There is a virtual integration. Separate value element like market information and analytics are merged to form value added

products. There would be competition from third party advisors like price comparison advisors. These firms are not deterred by legacy systems or overheads and costs on organizational structures. The established units would have to rely on advantages like customer base and a very well established information system. Additionally, they would also have a brand name. Further, there would be multi provider platforms, convenience and customized advice.

Today, barring a few banks in Sweden, Finland, Singapore and Japan, most banks are providers of hybrid services. It would be wrong to judge these firms with the criteria of new value propositions created, new business models developed or configuration of internal operations.

A development path can be envisaged for most banks along the lines of the three phases describe broadly as:

- Inflection.
- Evolution.
- Revolution.

The first two phases could see a strong upward thrust and growth due to the following reasons:

- Strong technical infrastructure.
- Aggressive migration initiatives.
- Scope improvements and price changes.

SECTION 3

At this stage, there is a threat to the universal banks as the customers would prefer institutions with a limited range of specialized products. There could be a period of sustained price competition and one might even see continuous price cutting. There is a distinct possibility of re-structuring of internal offline operations. It is certain that there would be a rapid expansion in brokerage and fund management institutions/sectors.

It can be safely concluded that the internet has made banking simpler and more convenient for those who have grown up with computers and who are 'time poor'. They can do their banking when and where it suits them. Limit set by geography and time has been overcome. Banks can look at the way their operations are conducted to see if the migration is really effective. Further, banks can also see if the large volume business migrates

to the internet. An equally important facet can be the development of products, which can exclusively be delivered through the internet only. The internet has opened a new frontier for businesses and invested banking with a new meaning.

So far, the broad criteria that banks can use to evaluate the efficacy of their technological upgradation efforts, have been discussed. However, far more important is the need to remove the most obvious weaknesses plaguing the system. It must be said that our conclusions are impressionistic and that they are based on experience narrated to us by staff members/users at meets, and so on. The major drawback is the lack of information about the facilities at the branch level. Somehow, the staff members are not aware of the facilities available or the rationale behind the installation. Emails received are not responded to even within reasonable time. Cheques are not cleared even for three days or so. High value instruments which should be cleared on the same day are rarely put through. The customers have to be alert and chase the concerned staff members to see that the amounts are received. Equally serious is the lack of any worthwhile effort at marketing of services. There is no attempt at differentiating the banks' services. The investments and the returns on them are left to themselves with the pious hope that they would pay for themselves.

The first question that needs to be answered is regarding the differentiation aspect. It is important for the banks to have a vision. There is no reason why banks should not think of having a pan-Asian customer base. To achieve such results banks need to have a single window service for bill payments, increase in credit card limits, transfer of funds, and so on, and all of these need to be handled through a single window. These things need to work intuitively by using standard navigation channels. Banks have to compete with the established leaders in the field and they must never forget that their customers have very high expectations.

Broadly speaking, some of the steps that need to be taken to achieve these results have been discussed below. There has to be a breadth of functionality and intuitive way in which the application behaves. It is easy to remember that differentiation comes through the following:

- Brand development.
- Wealth of information availability.
- Depth of transactional quality, underlying the products and services.

Businesses today need and expect a certain degree of tailoring of services. One such example is given here to bring home the point. Corporate

customers need different levels of services with varying authorization levels. They would like to nominate users with potentially different levels and with a built-in check for auditing what each level has done viz. 'check and release' transactions only if within user authority. One can never forget that corporate customers have different requirements than the average and less tech-savvy customer.

The proof of the pudding lies in eating. A case from Sweden or Korea needs to be used here to confirm that what has been said is not merely a castle-building exercise, but that such results can be achieved by banks. The case of Nordea bank has been discussed here to highlight the possibility of achieving such results. For the sake of brevity, a brief outline of the steps taken by these banks has been mentioned.

- It is necessary to start with the presumption that internet banking is a profit center activity. The result can be achieved through support from the branch staff. Otherwise, the goal can never be reached.
- Solutions attempted have to be simple, user friendly, secure and expandable.
- There has to be the same secure identification with each contact over each medium and terminal.
- Gradual introduction should be made to new product offers.
- E-banking has to be a part of the branch business.
- Corporate and other customers should get the same services.
- The branch staff must have a friendly attitude, and ensure prompt and timely response. Eventually, the staff would notice that customer satisfaction improves considerably.
- Be aware all the time that your competitor is just a click away.
- Profitability and payback on investment have to be in the forefront. Added value 'for free' is just not given.
- One thing is abundantly clear. Without staff support, e-banking cannot be launched and carried on as a profit center activity.

Risk Factors

The risk management policies for various activities like broking, banking and insurance shall be dealt with in a separate chapter. Some of the threats/risks, which impinge on the analysis made earlier have been indicated further:

54 E-finance

- Speed of technological change.
- Changing customer expectations.
- Increased visibility of public networks.
- Integration with legacy computer systems.
- Dependence on third parties for necessary technical expertise.
- Proliferation of threats and vulnerabilities in publicly accessible networks.

Management should review each of these perceived threats and adapt the risk management practices to meet the risks posed by e-banking activities.

The next section refers to the cases of stand-alone e-banks. We are of the view that sooner or later some of the mobile service providers are bound to enter this field. Non-bank finance companies would find this activity quite profitable when viewed as a supplement to their mobile telephone services.

Stand-alone E-banking

There are a number of banks today which regard the internet as a way to deliver the products; others see it as a separate line of business for the bank. Here, we would like to review the performance of the stand-alone e-banks. Let us first explore the possibility of a stand-alone internet bank. In course of time, the emergence of new entities in this field is a distinct possibility with newer approaches, work culture, and so on. For instance, a major telecom company like Reliance or a technology company like Infotech may decide to foray into this field and set up a stand-alone e-bank. Recently, *The Economist* published a review of the working of internet banking and concentrated on the reasons for their failure. Amongst the causes listed were: (a) customer resistance (b) expenses incurred on advertisement. The study no doubt highlighted the problems faced by the stand-alone banks. However, subsequent studies, particularly Robert De Young's (2001) work, does throw considerable new light on the working of stand-alone banks in which websites are the only delivery channel. Theoretically, low overhead expenses and access to larger geographical markets should allow better prices (higher deposit rates and lower interest rates on loans). It is true that in practice, they are struggling for profitability and they are not dominating traditional banks with branch networks.

It must not be forgotten that as e-banks age, they accumulate more experience. Experience effects have not been extensively measured in banking, though some recent studies do point to the fact that the performance

of banks improves over a period of nine years. De Young (2001) rightly points out that the maturity experience is important. As a new bank ages and its employees accumulate general banking experience, the maturity effect would transfer this experience into improved financial performance. This transformation occurs through improvements in numerous aspects of financial performance such as cost control, risk management, marketing or pricing policies.

There are two distinct possibilities. In the first instance, e-banks can draw on a talented pool of manpower available and make use of technology more effectively. There are areas where, even in large banks, technology is not being harnessed to the extent required. Stand-alone e-banks can handle areas like asset liability management, risk management or even investment management, more effectively because there would be less inter-departmental conflict. At the same time, these entities can experiment with the Drucker model. For instance, hospitals are being run by part-time consultants. In the same way, the core staff can be augmented by such consultants and the learning curve can be shortened. E-banks need to conduct their operations like start-up banks. They can also begin with broking, which is definitely a profitable activity, and then enter other business activities.

The second instance pertains to technology. The customers and some managers may take time to get used to the new technologies, they would eventually have an edge over others in translating this into an improved financial performance. With the scale of operations changing, the technology effect transforms into improved financial performance through a reduction of unit costs.

De Young has in his study, compared the performance of newly established banks with newly established banks with branches. The analysis shows that on a purely static basis, newly chartered internet banks perform poorly compared to newly chartered traditional banks. The dynamic analysis suggests that the performance improves more quickly over time at the internet-only start-ups and the evidence is consistent with both technology-based effect and technology-scale effects (see Tables 5.1 and 5.2).

Most banks that use the internet-only business model are struggling for profitability and it may lead one to conclude that this model does not seem to be a particularly successful one. But the study also shows that profitability ratios and non-interest expenses ratios improve more quickly over time at the internet-only start-ups than at the traditional start-ups. If these trends continue, the internet-only business model could prove to be a viable business proposition.

Table 5.1 Internet and Non-internet Banks—A Dynamic Analysis

<i>Dependent Variable</i>	<i>Static Analysis</i>	<i>Dynamic Analysis</i>	
Return on Assets	0.0310	0.0094	0.0078
Return on Equity	0.1096	0.0123	0.0006
Interest Margin/Assets	0.0002	0.0004	0.0005
Equity/Assets	0.1034	0.0334	0.0126
Non-interest Expenses	0.0214	0.0158	0.0148
Premises Expenses/Assets	0.0015	0.0008	0.0013
Labour Expenses/Assets	0.0045	0.0047	0.0084
Wages (full time employees)	0.0083	0.0022	0.0014
Non-interest Expenses/Assets	0.0154	0.0104	0.0053
Depreciation/Assets	0.0700	0.0417	0.0381
Loans/Assets	0.0636	0.0208	0.0331
Non Paying Assets (NPA)	0.0000	0.0000	0.0006
Asset Gross Rate (annual)	0.7524	0.0086	

Source: De Young (2001).

**Table 5.2 Internet and Non-internet Banks—Selected Balance Sheet Ratios
(a) Loan Comp. (b) Funding**

<i>Asset Size Category</i>	<i>Deposits/Assets</i>		<i>Purchased Funds/Dep.</i>		<i>C & I Loans/ Credit Cards Loans</i>	
	<i>Internet</i>	<i>Non-internet</i>	<i>Internet</i>	<i>Non-internet</i>	<i>Internet</i>	<i>Non-internet</i>
Less than \$100 mn	20.4	16.9	0.5	0.4	82.1	85.1
\$100 mn to \$1 bn	17.9	18.1	1.7	0.9	78.9	82.3
\$1 bn to \$10 bn	24.5	17.8	4.2	0.9	68.6	71.8
\$10 bn and over	34.1		2.8		66.1	11.7

Source: De Young (2001).

There is one question, which remains to be resolved. It is now clear that the earlier fear of brick and mortar banks vanishing like the dinosaurs is not a possibility in the near future. Thus, why should the management not increase its geographical spread? The option is not only open to them but also a viable one. An analysis of key ratios of their respective balance sheets shows that the brick and mortar branches do perform better than branches of internet banks.

It cannot be ruled out that there is a fairly high degree of scepticism about the viability of e-banks. The reasons for this stem from the fact that these banks have not been performing as well as they should have. For example, the entry of the most successful 'pure play' internet bank 'EGG', was dramatic. It developed a customer base of 150,000 customers and 1.3 billion pounds sterling in deposits. In the first three months, it had over a

quarter of a million customers and deposits of 5 billion pounds. The customers were not only affluent, but also technology literate. It had a very substantial share of mortgage loans. It was hailed as a great success story. EGG was widely hailed as a strategic triumph that revolutionized British banking and the most extraordinary success story in new customer acquisition retail banking has seen. However, underneath it lay the faulty banking policies. It offered a savings rate that was higher than the prevailing market rates which meant negative deposit margins and in effect giving money away.

So although it initially did succeed in scaling dizzying heights, did it make money? Would it make money over a period of time? Not in the near future given the accumulated losses. What banks lose in higher deposit rates can be made good by maximizing the price or rates at which they lend. However, it is doubtful if one can lend at rates higher than the market rates. The competitive dynamics of the market place will force prices down to gain sales at the cost of margins. For standardized, low risk products such as mortgages, competition is severe; no bank can afford to charge more. For high risk, unsecured lending, risk should be the main consideration. The primary determinant should be risk not merely competitive margins. Traditional banks have one more bow to their string, that is, the fee income. Unfortunately, many internet banks waived such fees.

In the aforementioned business 'model', it would be difficult to make profits. This is exactly similar to other low margin businesses. Scale is the only way out. To build scale, requires a relentless focus on attracting customers whatever the cost (which leads to lower margins). The bank gets into a vicious circle of destruction of profits.

Questions regarding the high costs incurred by banks are often asked. Since traditional banks have high cost structures (translating as poor cost discipline), it is suggested that the protected environment of domestic banking has given rise to inefficient dynamics of domestic banking.

On the other hand, the internet banks have low costs. It should be possible for them to offset the 'losses' elsewhere. These banks would make their money on super low operating costs. It is, however, clear that lower margins and lost fee income cannot be made good by a low operating cost. Nor is the influx of high net worth individuals with an idle balance in the account able to offset the fundamentally flawed 'economics' of business. In an article in the *Asian Banking Journal*, (2000) Scott Roman estimates 'that these Banks would have to triple the average balances of their customers or further reduce costs by 47%.' Clearly both these options would be difficult to exercise.

The only option, and it is not an option, but a fundamental necessity, is to start pricing sensibly. The logic of banking business demands that breaking the fundamentals of business is not a feasible proposition. Rather, adherence to the basics alone can protect 'shareholder' value.

The problem gets compounded when we note that the size of the market is considerably small and growth can be at the expense of another institution. Marketing then amounts to 'poaching'. Obviously, a price is extracted for such a transfer.

The lesson is that pure play internet banks must decide whether they are looking at themselves as 'business entities' or as delivery channels. This would affect their marketing strategies as it could lead to a situation where banks become desperate to be available on the internet, but neglect to persuade their customers to choose their facilities. Many banks do not offer an incentive to bank on the web. Customer emails were not responded to even after a lapse of 8–10 hours.

Mobile Banking

Reserve Bank of India has issued certain guidelines on banking services being availed of through mobile access devices. Apparently doubts have been raised about the security aspects and the RBI has advised banks not to proceed any further in the matter of mobile banking services. Currently, the RBI is reviewing the regulatory aspects and banks have been advised to proceed further once the review process is duly completed. However, it would be worthwhile looking at the experience of Korea or Japan, where the preponderance of mobile banking users could be a guide for Indian financial institutions.

Equally important are other allied developments in Japan. There is a proposal to form an entity exclusively for providing mobile banking services. Some banks are getting together to form such an entity. In India, there is a distinct possibility of mobile operators forming an alliance with an Indian bank to set up such a venture. It is equally likely that technology modifications would permit an access through the mobile devices. After all, one has to reckon with the small size of the screen. Surely, one would not be looking for a loan application through this medium. Perhaps, the use could be restricted to getting quotes, status reports on accounts or getting alerts.

The technology breakthrough which people are waiting for is to have a chip which could be used to access accounts with different banks. It is expected that sometime during 2009–10 should see this facility being

made available. Banks are not particularly happy over such a development because of security concerns.

A broad spectrum of developments have been outlined and India's low costs for technology development should give it a great advantage to steal a march over some of the struggling banks overseas and get to their clients and to attract them.

E-INSURANCE

E-insurance can be broadly defined as the application of internet and related information technologies (IT) to the production and distribution of insurance services. In a narrower sense, it can be defined as the provision of an insurance cover whereby an insurance policy is solicited, offered, negotiated and contracted online. While payment policy delivery and claims processing may all be done online, technical and regulatory constraints may not allow these elements to be subject to full e-commerce application in certain countries. However, insurance legislation is being continuously modified to accommodate online payment and policy delivery, and outside the discussion of e-insurance metrics, these elements should be included in the narrow definition. In India, for instance, Insurance Regulatory and Development Authority (IRDA) has not yet permitted insurance companies to use the internet as a distribution channel. But premium calculations can be got done on the internet and in some cases where risk has been assessed, renewal premium can be paid.

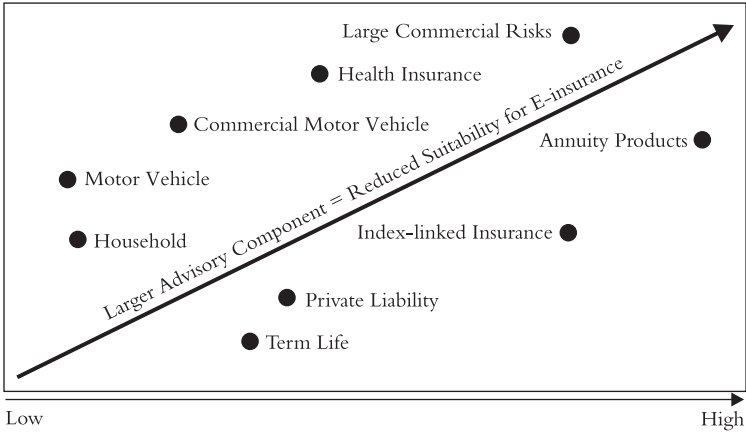
To ensure legality the client needs to have an insurable interest and the asset to be insured has to be the property of the client and some information confirming this is usually submitted. The condition of offer and acceptance is satisfied by having the insurer offer coverage terms and conditions for an insurable interest, against a loss caused by general or named perils under particular conditions of hazard. The client reciprocates the offer by expressing an acceptance of the proposed contract. Consideration for an insurance contract assuring payment or compensation for the loss event is the receipt of insurance premium. The promise is a non-physical information service. Similarly, the transfer of funds is often electronic and even cash itself has a nominal value unrelated to its physicality. When a loss occurs, the damage is assessed and a claim is submitted. Large amounts of data are again transmitted between policyholders, intermediaries and insurers—insurance requires modern e-commerce legislation that permits insurers and the insured to safely and unambiguously exchange information, make electronic payments and validate their responsibilities through digital signatures.

At this stage it needs to be pointed out that there is a marked reluctance amongst insurance clients to complete insurance transactions through the internet. Most of the insurance companies have either centralized data storage or are in the process of building it up and soon many of the transactions including claims settlement could be centralized. Even the Life Insurance Corporation of India would be able to settle claims arising centrally. Once that happens we see that the move towards e-insurance would gather momentum. Further use of handheld devices would facilitate offering services to the clients electronically as the agents could perform the role of ‘Aggregators’.

Prior to concluding the insurance contracts, a good deal of information is required to be submitted to the insurer. To do so via the internet might pose difficulties and it would be cumbersome to verify the same (see Figure 5.1).

Before we examine the possibility of internet being a viable distributive channel it is necessary to understand the current environment of the insurance sector. For the last few years, fears about the soundness of the insurance sector were expressed by various regulatory authorities. The latest AIG debacle has raised questions about the sector’s basic viability. The life and non-life segments have been affected by placing too much emphasis on the small print of the contract, dubious policies of surveyors, hospital authorities, third party claims settlers and service providers. The

Figure 5.1 Product Complexity



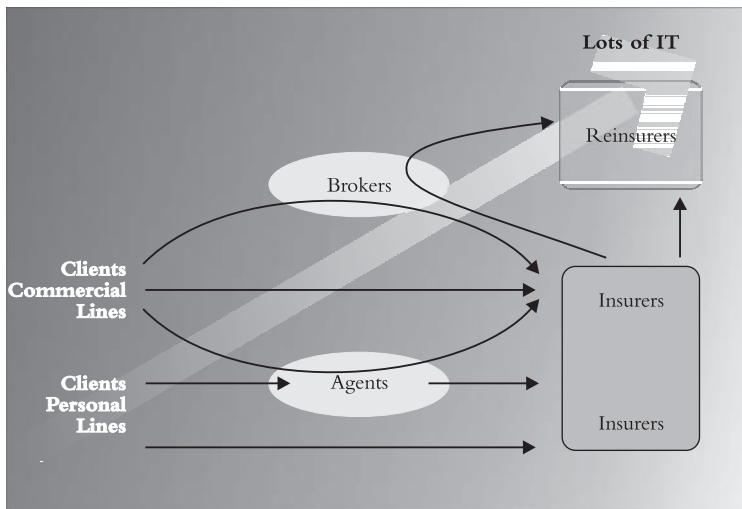
Source: E-Commerce and Development Report 2002.

insurance industry will have to lift itself by its own boot straps before it could claim to attract genuine clients and to meet their requirements. They have to clean up their sullied image. Last but not the least, is the investment aspect. The investments made are risky, highly speculative in nature and activities undertaken with an eye on bonus payments to the staff. The result is the fate of AIG.

In view of the current legal requirements, use of e-insurance would essentially be a PC-based activity. Cross-border activities, if any, are likely to be perhaps restricted to regional groupings that may emerge. It is, likely that in the rural and micro finance segments the vacuum currently felt may be filled by postal insurance, which has a distinct place in mobilizing savings. The use of electronic devices by the postal staff and provision of internet services through the post offices would enable them to get a hold in this market as never before. Perhaps, the regulatory changes that are likely to be ushered in after the present debacle would lead to modifications to legal aspects and facilitate the transition to a more healthy sector. Then the newer distribution channels could bring the customers in direct contact with the companies. The present broker dominated agency system would have a sway for some time to come.

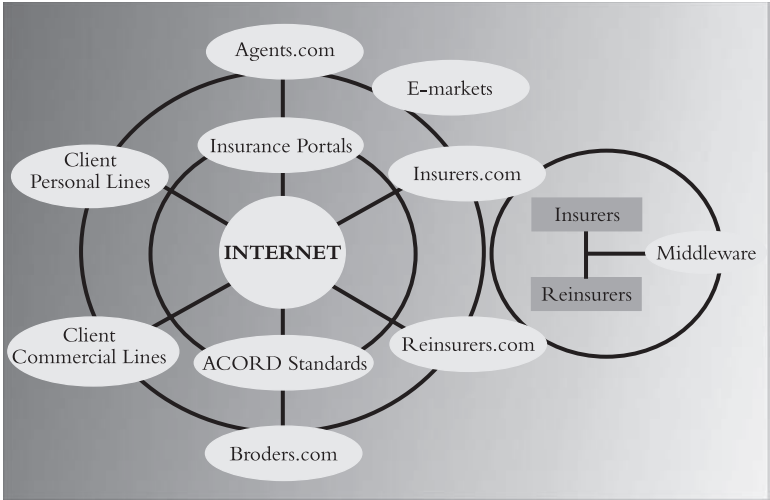
The possible changes that can come up if IRDA allows companies to use the e-distribution channel have been represented in Figures 5.2 and 5.3.

Figure 5.2 Pre-internet: Insurance



Source: *E-Commerce and Development Report 2002.*

Figure 5.3 Internet-enabled Insurance



Source: E-Commerce and Development Report 2002.

E-trading

In the first edition of this book our thrust was on detailing the procedures and practices adopted in the new distributive channel. There was a degree of novelty about the mechanism and the number of transactions was not significant. However, the last three years witnessed a tremendous upsurge particularly in the shares trading and introduction of trading in Government of India (GoI) securities and currency trading. The introduction of newer products could certainly be regarded as an additional stimulus to the growth process.

The current financial crisis has, however, pushed the hands of the development clock several notches and a very promising area of development (both for theoretical work and the resultant applications) has received a considerable setback. The removal of capital adequacy requirements and relaxations offered to the leading investment banks by the SEC (securities and exchange commission) in the US resulted in their ultimate downfall. The staggering losses recorded are a sad reflection on greed and avarice leading to their demise. Some US entities have ceased to exist as investment banks. Further, the future is so bleak that at this point of time it is difficult to see technology upgradation and innovation playing a large part in changing the rules of the game or leading to other market developments. This may appear as a mere reiteration of what happened but hopefully should serve as a guide for revival on the lines seen earlier. Recently it has come to light that some large-sized firms have been using 'Super Computers' to undertake trading. It has given them advantages (some would call it pure misuse of technology) in undertaking profitable trade deals. One would like to have this practice regulated. Otherwise only the large players would be able to offer services and any technological

advantage that now accrues to these firms would no longer be there. The field would then be solely dominated by very few firms. This is indeed a truly undesirable change.

This chapter focuses on the impact of the changes not merely on business volumes or commissions charged, but also looks into the wider questions of process of intermediation, competition, exchanges and trading systems, clearing and settlement systems, legal and regulatory frameworks, and so on, as later when the system shows signs of improvement, one could have a holistic approach in dealing with these issues. The term e-trading can be described as follows.

The term ‘electronic trading’ encompasses a wide variety of systems, ranging from simple order transmission services to full-fledged trade execution facilities. We, therefore, define ‘e-trading’ in a somewhat broader context. It is a facility that provides some or all of the following services:

- Electronic order routing from users to the system.
- Automated trade execution—translating orders into trade.
- Electronic dissemination of bid/offer quotes and depth.
- Post-trade information (transaction price and volume data).

It is necessary to cover in this definition even those systems, which do not include trade execution facilities. The purpose here is not to examine a system, but to look at e-trading in general and its impact.

Compared to the earlier systems, e-trading has certain advantages and these need to be highlighted before we go into a detailed discussion of the other aspects listed earlier. It would be useful to point out that electronic systems differ from traditional markets in several respects. The use of computer, automates aspects of the trading process and changes the relationship amongst dealers and customers. The effect, however, is not to build a better telephone, but to create a new way of trading different from either floor-based or telephone-based trading. The point we are making could best be illustrated by highlighting the differences (particularly those that are noteworthy).

- E-trading is location neutral.
- It allows multilateral interaction and that too on a continuous basis.
- E-trading is scalable. Electronic systems can be scaled up to handle more trade simply by increasing the capacity of the computer network. In traditional markets, the size of the floor has to be

physically expanded or the number and capacity of the intermediaries has to be increased. The scalability can enhance the reach of the dealers through a greater access to a widening base.

- Operational costs under the ET system can be reduced because economies of scale can be exploited.
- E-trading is integrated. It allows straight-through processing by integrating different parts of the trading system.

The tremendous growth in the volumes of business on the internet has had a number of consequences. It was also felt that there would be structural changes and that the first causality would be the elimination of intermediaries and an end of the brick branches of broking houses. However, there is no let up in the physical presence or the branch network. The model currently in vogue is the brick and click one. Perhaps it is not wrong to say that most stand-alone broking firms find it necessary to develop a physical presence too.

It is now possible that even trading with the help of cell phones would be permitted. However, it is necessary to clearly bring out that there are a few security issues related to mobile trading, on which SEBI seems to be working. There should be no risk of hacking. Also, we should guard against the mobile phones falling into wrong hands. We are geared up with technology, which also involves readiness on part of brokerages and telecom service providers to start mobile trading. Sudhanshu Verma, chief executive officer, Asian CERC Information Technology providers, along with brokerage houses, is also looking forward to meet SEBI officials to sort out the issues. There are few protocols for mobile trading such as SSL certificate in online trading, which ensures the security level of a particular transaction. These matters are currently being looked into by SEBI. The market regulator had allowed net trading in 2000, where upon, the number of trading participants grew significantly, but volumes did not match the growth. At present, mobile services at brokerages are merely seen as a value-add through which customers are given basic stock information.

We are having the basic infrastructure in place, once the SEBI guidelines come, the technicalities would be completed and mobile trading could start. As compared to online trading, mobile trading could boost trading participation, as the latter is much more flexible and easy to use. (Amit Golia, head, E-Broking, Motilal Oswal, Press Report)

Recently, the Bombay Stock Exchange also launched its Mobitrack service, which allows the user to access stock price details such as last traded

price, change and percentage in each scrip, besides giving information about profile of few specific scrips selected by the user. Vinay Agarwal, executive director, E-Commerce, Angel Broking, feels regulations for mobile trading would be more or less similar to online trading as security-related issues are already addressed in the internet trading guidelines. 'I don't think there is much of an issue with security as we have already implemented the online trading successfully,' he said.

A review of the intermediation process is important at this stage. The current theoretical work is directed at embracing traditional intermediaries and markets in one framework and the new approaches/perspectives would enable us to have a better understanding of the system.

The theory of financial intermediation is based on the classical assumption of perfect markets. According to this view, intermediation exists because of market frictions and imperfections and remedial measures are taken by the intermediaries. The impact on costs and the importance of asymmetric information between investors and borrowers is stressed to highlight the role of intermediaries. One, however, feels that this is perhaps too passive an explanation of intermediation. The growth of financial markets and technology changes have dramatically brought down the costs and alleviated information asymmetries. The intermediaries have not only survived, but are in fact growing in strength. This has led to some modifications to the age-old views about intermediation. It would perhaps be right to say that the intermediaries are not merely undertaking matching functions, but are also undertaking other activities like creating and testing new products before they are seasoned enough to be traded in a financial market. A review of literature prior to the current developments suggests that the old assumptions of perfect markets are being discarded, and that more and more financial institutions are being viewed as independent parties, which create products and whose worth to the clients stems from transformation of risks, term, scale, location and liquidity. Perhaps, the future would view the market as a microstructure. The focus here is on how markets are created and how they function. They put the market mechanism under the microscope and analyse specific institutions of exchange, trading rules, price formation, and so on. They also study the impact of information on prices. One could describe the nature of the work done as integration of developments in economics of information, rational expectations and imperfect competition. This information-based game and theoretic paradigm models are the basis on which further developments would have taken place had the system not received the jolt that it did. The shape of current theoretical work in these areas is somewhat hazy.

There is some discussion about the efficient market hypothesis, etc. But the other aspects are not getting the attention they should. The whole context is changed and one would have to wait before making generalizations on important aspects of market developments. At this stage any guess is as good as any other. It is important to highlight that the screen-based trading and settlement system put in place by the Clearing Corporation of India for Government of India Securities has virtually eliminated the broking system in gilt-edged securities.

The behaviour of banks and more particularly of the investment banks and their dealers during the crisis has played havoc with the established rules of the game and has made it necessary to reiterate the basic requirements of a sound trading system under free market conditions. The suggestion that they were economical with the truth may make a sound copy in a newspaper, but one can never forget that it brought the system to the brink of disaster.

TRANSPARENCY

The question of transparency is also important. It can be defined as the public disclosure of reliable and timely information that enables the users to assess a unit's financial position and performance. To achieve transparency, the institution must provide accurate, relevant and quantitatively and qualitatively sufficient information on a timely basis. When applied to e-trading it assumes certain additional dimensions and these could be well brought out by a reference to a directive issued by the European Commission in this behalf. It would not be wrong to say that this whole question needs to be handled with utmost care as any 'leaks' about large trades could have adverse impact on the price sensitive issues. Equally important is the transmission of information likely to affect the overall market conditions.

It can be said that the approach adopted by the European Union's Financial Market Directive (MIFID)—Article 65, affords a very practical solution to the problem. However, special efforts are necessary to restore the balance and semblance of orderliness. Perhaps, the solution lies in having a framework as visualized by the commission.

Broadly speaking, the pre-trade transparency requirements in MIFID in respect of shares require regulated markets (RMs) and multilateral trading facilities (MTFs) to publish current bid and offer prices for shares and the depth of trading interest at those prices. MIFID also requires

investment firms who are ‘systematic internalisers’ to publish firm quotes in liquid shares, which they systematically internalize. In terms of post-trade transparency, MIFID requires RMs and MTFs to make public the price, volume and time of the transactions executed under their systems in respect of shares which are admitted to trading on an RM. Investment firms that conclude transactions in shares outside of an RM or MTF must also make public information relating to those transactions.

PRE-TRADE TRANSPARENCY

Indicative or Tradable

Prices/Indicative or Tradable Quantity

Prices can either be indicative or firm, tradable prices. If they are indicative then you could usually contact a dealer to obtain a firm and tradable quote. Prices on exchange-traded markets, such as an exchange’s order book, are usually firm prices, but prices in Over the Counter (OTC) markets are usually indicative. One must be able to see the depth of interest in trading. On exchange order books, you can usually see the volume of a security, investors are willing to buy and sell at various prices. In OTC markets you may just see that prices are good for up to certain volume, but if the investor wants to trade in larger size, is the information made available on a real-time basis?

Price Quantity Real-time or Delayed

Publication

The prices at which trades have been executed and the size of executed trades need to be published as quickly as possible. In some markets, the size of trades may be subject to some disguising such as indicating that the trade was in excess of a certain threshold. In others it may be the full amount of the trade. Is the information about trading updated instantly or is publication delayed? The degree of delay may depend on the size of the trade.

There is one aspect, which has been attracting the attention of security agencies, authorities, and so on. It is the misuse of these channels by rogue traders/terrorists and hush money peddlers. Normal trade practices and instruments can be put to absolutely perverse ends. Equally worrying is the fact that institutions, themselves, hide their exposures and try to portray a

totally wrong picture by not disclosing the risks. Frankly, one is faced with a peculiar situation here. Bigger the institution the greater is the danger of a contagion effect and the impact on the whole system.

INTERNET TRADING (E-TRADING) IN SHARES

When SEBI allowed e-trading, it was expected that brokers would rush to the websites and trading through websites would increase. On the internet, one can trade instantly and transparently from any part of the world. These expectations have actually been fulfilled. The current market scenario may have dampened the overall activity, but the infrastructure is in place. Trade is confirmed and one could have the rate, the time at which trade took place and even the name of the counter party, and so on. Thus one could be doubly sure about the authenticity of the transaction. There are quicker settlements and collections.

ELECTRONIC FUND COLLECTION

Under this system, the brokers get their funds directly credited to their accounts and the clients can in turn get their accounts credited or debited. This facilitates quicker payments, improves the liquidity position of brokers as he gets funds one day after the payout day. This obviates possible defaults or cash out positions of brokers and sub-brokers.

The website on the basis of investor's portfolio can give him information on the company's results, performance, report cards and company analysis. There will be a number of improvements in the process as well as the products. So far as the process is concerned, there will be settlements on a daily basis and on a rolling basis, electronic settlement and clearance, email for transmission of funds. As far as product improvements are concerned, portfolio of investors may include a number of new products such as derivatives and synthetics (see Joshi and Joshi [2009] for a detailed note on synthetic securities).

The other facilities include basket trading, trading in index funds, voting and non-voting shares, tracker shares and complex derivatives. Tracker shares refer to the separate divisional shares of a company such as IT divisions of Wipro or Tatas. The portfolio tracker for valuation can do so by clicking on to a company/broker website for company analysis and MIS on the companies in one's portfolio represented through the website. There will be automatic borrowing and lending facilities institutionalized

security lending, automatic financing or margin buying and a host of other facilities on the stock exchanges.

E-TRADING IN FIXED-INCOME SECURITIES

Initially, fixed-income trading was slower to exploit electronic platforms than equities markets. That is because fixed-income markets are very different. In contrast to equities, fixed-income markets provided no opportunities for arbitrage—the simultaneous purchase and sale of the same securities in different markets to profit from unequal prices—because the securities are seldom quoted on multiple markets. Further, the broking system was so deeply entrenched that it was difficult to break the sway they had over the entire system. Electronic trading of fixed-income securities enables investors to secure instant access to all the relevant information about security being traded. Finally, electronic trading could increase efficiency and lower trading costs, particularly for small and odd-lot transactions. Retail online trading in Government of India (GoI) securities through stock exchanges became a reality, when the then finance minister, Jaswant Singh, made the inaugural purchase of 10 units of 11.10 per cent paper with face value of Rs 100 each, that was supposed to mature in April 1995.

In the process, a new milestone in the history of the country's capital markets was achieved, opening up trading in Government Securities—hitherto confined to only banks and institutional players—to retail investors, who can place orders for as low as Rs 1,000. So far, the only option for the retail investor was to approach a primary dealer, who would book orders on his behalf through the Negotiated Dealing System of the Reserve Bank of India (RBI). Further, the investor had to commit himself to a minimum amount of Rs 25,000.

Electronic trading of fixed-income securities enables investors to secure instant access to all relevant information about the security being traded. Finally, electronic trading can increase efficiency and lower trading costs, particularly for small and odd-lot transactions.

Generally, electronic platforms, which compete against single-dealer platforms, are of several types:

- Auction or bidding systems that allow dealers and investors to bid directly on new issues.
- Multi-dealer systems that allow institutional investors to trade with dealers, but not with each other.

- Cross-matching systems that allow buyers and sellers to trade or periodically match orders anonymously.
- Inter-dealer broker systems that allow dealers to trade anonymously with each other.

As the number of trading and dealer platforms has increased, financial institutions have conducted arbitrage within single markets by identifying pricing discrepancies.

The aspiration of the major platforms must be to become the market, through the scale of deal flow, such that they provide real trading connectivity between the various fixed-income markets. In the longer term, the result will be consolidation of some of the fixed-income markets as has happened in equities markets. In India, the Clearing Corporation of India has now developed such a sophisticated system that the daily trade and settlement takes place in real time and the system is rated to be almost as good as available in more developed markets. The investor can trade in Government Securities in demat form across 10,000-odd terminals of the three designated stock exchanges—National Stock Exchange, Bombay Stock Exchange and Over the Counter Exchange of India. The settlement cycle has now been shortened to T+1. The minimum order size, keeping in view the small retail investor, has been pegged at 10 units (each of Rs 100 face value) and multiples thereof. To begin with, all outstanding and newly issued GoI securities will be offered for trading in the ‘automated, anonymous, order-driven’ system.

The RBI will provide the designated exchanges and depositories a list of securities that can be traded. Retail online trading in treasury bills, state government securities and other approved securities will also be permitted in a phased manner by the RBI, in consultation with the Securities and Exchange Board of India (SEBI). The RBI has decided to extend electronic trading in gilts—the screen-based anonymous order matching—to insurance companies. By the end of September 2005, 117 members were active on this module. NDS-OM volumes covered around two-thirds of the total outright transactions in dated government securities in the secondary markets.

The insurance companies have now been permitted to participate in the screen-based trading system. The Managing Director of Life Insurance Corporation (LIC), Mr D.K. Mehrotra, said that allowing insurance companies to participate in the debt market would bring about ease in transactions. It is especially useful since confidentiality is maintained and our quotes are kept anonymous. According to sources, insurance companies,

including LIC, had sought the move towards screen-based order matching since it provides for less price manipulation, minimum impact cost with quotes being availed of on a real-time basis. Mr Puneet Nanda, CIO, ICICI Prudential Life insurance said, 'Our company has a large asset-base of over Rs 5,000 crore with substantial investment in G-secs and a move like this would bring it at par with other institutional players.'

We now look at the corporate bond market. So far electronic trading has not been permitted in corporate bonds. It is likely that there are apprehensions about the complex products that are likely to hit the market. Bond investments are not always a suitable investment for retail investors. The diversity of the bond market is an important consideration here. While it is undoubtedly true that many bonds are effectively credit risk-free investments on the grounds that the borrowers, particularly governments and supranational organizations, are extremely unlikely to default on their obligations, many other bonds bring significant credit risk and may not be suitable for all investors, who may not understand the level of risk they are exposed to nor have the financial standing appropriate for such investments. Similarly, the interest rate risk associated with such bonds may mean that they are not suitable investments for retail investors. Perhaps the 'Wall Street Devils' have queered the pitch to such an extent that it may be sometime before bonds trading takes roots in any significant manner.

FOREIGN EXCHANGE TRADING

The Clearing Corporation has now made it possible for forex transactions to be routed through the internet transactions. Major developments, including derivatives trading, would have taken place after the regulatory issues were sorted out. A joint mechanism needs to be in place. We would begin with the list of new products approved in principle by the SEBI Board (PR No. 297/2007). Further, the RBI and SEBI standing committee on exchange-traded currency futures (RBI 2008) and the comprehensive guidelines on derivatives are extremely useful. Somehow, there are a whole lot of unsettled legal issues and these have led to a number of court cases being filed against the banks, and so on. These are naturally impacting the developments. The mechanism for undertaking the transactions is certainly in place and these could easily be done through the Internet.

The SEBI Board sanction covers the following products relating to:

- Mini-contracts on equity indices.
- Options with longer life/tenure.

- Volatility index and F&O contracts.
- Options on futures exchange-traded currency futures and options.
- Introduction of exchange-traded products to cater to different investment strategies.

In conclusion it can be said that Clearing Corporation has amply demonstrated that these transactions could safely be put through on the internet and complete anonymity regarding the deals would be maintained. The concerned banks/organizations need to make sure that their back office mechanisms, clear-cut demarcation of duties are in place. Last, but not the least important are the risk management systems.

Click and Brick Marketing

For quite sometime there were a few banks (Citibank, HSBC, HDFC, and so on) which made services, such as viewing statements, operations on accounts and/or broking services, available to their clients. Discussions about marketing for services on the internet tended to be academic. However, a large number of banks, both large and medium sized, are providing these services or are preparing themselves to provide such services. Additionally, all these banks have adopted what could broadly be described as brick/click model. The reasons for having the provision of internet facilities are largely grounded in the banks' business requirements. The transaction costs are very high and levying service charges which compensate them for the services rendered is not a feasible proposition. In fact, the then Governor of the Reserve Bank of India frowned on the banks' costs and cautioned against such costs. Equally important is the realization that the younger generation is tech savvy and that they happen to be the wealthier clients whom the banks could ill afford to ignore. The competitive forces are too strong to be ignored; ignoring such groups could only be at the bank's own peril.

Having invested substantial amounts in technology upgradation banks have to ensure that their objectives are well achieved. It has to be asserted that successful strategies need to be built around customers. They have to evolve a framework that meets customer needs. Competing on prices and products would not be enough. The only tool available would be customer service, reliability and trust. We would, therefore, go into the theoretical aspects and then conclude with a few illustrations drawn from the working of a few banks, which has achieved a degree of success.

A major stumbling block in persuading clients has been a lurking fear that these distribution channels are not secure. They are susceptible to crimes

and that banks would try and pass the buck to the clients. Further, the crimes are not localized and that one faces great risks in using these services. It is important not to underestimate the dangers lurking in internet services. However, we must not exaggerate and avoid use. There are such dangers even in paper transactions. Frauds, misuse of bank funds, and so on, are somewhat inherent to the system. Banks must, therefore, educate not only their customers but even their staff members about the advantages of such use and educate the customers about the care that should be taken while using these facilities. Merely having formal agreements which are primarily to safeguard the banks' or FIs' interests are of no avail. Marketing efforts in the initial stages will necessarily have to be concentrated on educating the customers. One is reminded of the days when rural customers had to be introduced to the banks and the services they offered.

Despite the wealth of evidence that information and information technology are rapidly transforming almost all phases of economic and business activity, relatively little formal attention has been paid to the effects of transformation on marketing theory and practice. Due to the dearth of academic empirical work in this area till date, most of what is known about the information environment and marketing comes from rapidly accumulating evidence and documenting corporate experience.

The speed with which information is transmitted, the amount of information that can be stored and the ease of creating patterns of organizing information, are giving rise to qualitative changes. The key variable is information itself. The value of information depends on facilitating exchange within the value-added chain, down stream, between the firm and the consumer; and upstream, between firm and supplier and within the firm itself. Conventional marketing activities are transformed because the World Wide Web presents fundamentally different activities than traditional media. The transformation takes place because traditional methods cannot be easily implemented. Non-verbal communication is deconstructed with the use of 'emoticons'. Once you include the consumer, the goal of marketing could move from satisfying customer needs to inclusion of an altruistic, cooperative goal of facilitating the development of the market itself.

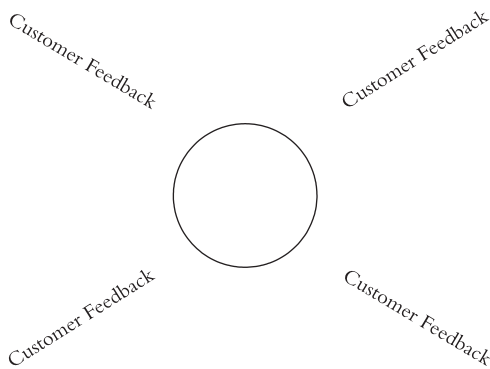
Traditionally, effectiveness of an advertisement campaign was judged by customer response. The same logic was applied to advertisements on the internet. The number of hits (accessed by internet users) was looked on as an indicator for judging the effectiveness. A number of 'theoretical' models were developed to forecast the possible outcomes of advertisements. These, however, proved to be elusive as the basic premise on which they were based was incorrect. Mere hit/click did not mean much. The one too many models used in theory and practice of marketing has only limited utility.

The web, in course of time, would change consumers' role as receivers of marketing information and would allow them to be active participants.

The focus during the early stages of the electronic revolution has been squarely on technology. Discussions are centered around access devices, software vendors, hardware platforms and specific joint ventures or platforms. A critical component has been overlooked and that is the marketing of these products. Perhaps, it may be complacently assumed that the product would sell itself. This unfortunately may turn out to be wishful thinking. It should be mentioned that there is no consensus view concerning the most effective approaches for marketing electronic products and services. Most banks have hardly any experience (except perhaps ATMs).

The nature of the problem must first be identified. The biggest challenge here is to provide the customers the breadth of choice they demand. The customer is now in the driver's seat—refuse customer a loan today and he/she would find numerous others willing to provide the same. Charge them interest for being overdrawn and they would move to one that does not. The brick/click model requires a well-thought out marketing plan, which would satisfy both the internet customers and those wishing to avail of branch networks. In fact, quite a few customers could be in both the categories. Equally daunting is the task of ensuring a service level to which internet customers are accustomed. A mismatch between promises and practices or procedures, could have serious consequences. For the last few years, banks and financial institutions have been so preoccupied with their internal issues, that customer service received short shrift. The industry's propensity to raise fees to boost non-interest income has not helped either. It is time indeed that banks paid utmost attention to customer feedback (see Figure 7.1). The next bank or financial institute is only a click away!

Figure 7.1 Customer Service



Source: Prepared by the author.

MARKETING FOR INTANGIBLES

Before proceeding further an examination of some of the fundamental changes that have occurred, with regard to 'intangible' products is important. In the 'new economy' exchange of information is not a by-product, but a central activity of financial markets. Information-driven dynamics of modern financial markets needs to be thoroughly understood. Perhaps one needs to modify Toffler's three waves and state them as under (see Toffler 1990–92a).

In the agricultural economy, there was a relationship between man and nature or natural products. In the industrial economy the focus shifted to man and machines and machine made products. The intangible economy is structured around relationships between man, ideas and symbols. We now live in a 'weightless economy'.

How does one comprehend the digital economy? The demand and supply sides need to be carefully considered. The demand for intangible artifacts and the supply of intangible assets such as brands, intellectual property and human capital could help in understanding the nature of these 'products'. These intangible products include, amongst other things, different forms of information and communication, audio and visual media entertainment and leisure, as well as finance.

Normally, these are joint products which are nondestructive or nonsubtractive. For instance, you might have recorded a song on a tape. Replication technology now makes it possible to have the same on CDs, DVDs, and so on. One can replicate and have as many tapes as one wants. Additionally, the same content may support a number of artifacts. Knowledge, as the ancient seers suggested, increases through imparting. The cost of sharing these is nil. The owner of an artifact cannot prevent/limit its consumption without paying for it. The earlier equation that purchases equal consumption is no longer valid. The number of free riders routinely exceeds that of paying consumers by a factor of three. Further, the consumers create their own combination of content.

The most important fallout is that conventional pricing and transaction mechanisms largely tend to be inadequate. Economics of scale are determined by consumption and not by production capacity. There is a further problem regarding information. Prof. Stiglitz calls it 'infinite regress' (Stiglitz 1985). It is impossible to determine if it is worthwhile obtaining a given piece of information without having this information.

Earlier, the pricing of intangibles was based on support. The price of a book was determined by printing quality and thickness. Now, content can be disassociated and priced separately. In financial services, equity research

is bundled into brokerage commission. The range of pricing is getting broader and more complex. Further, depending on the supplier–consumer relationship, different pricing arrangements can exist. The internet is really a fascinating laboratory for selling, sharing and giving away. These vary from metred charges, fixed assessed charges or charges for ancillary services.

On the supply side, the greatest importance is attached to brand management. Apart from brands, there are intellectual property patents and trade-marks that are critical competitive weapons. Curiously enough, these are not seen on the balance sheets. Reuters acknowledges that its balance sheet does not include factors such as its neutrality, software, intellectual property, global database and skilled workforce.

Even successful products could be replaced or could coexist with otherwise what may be called the ‘book store effect’. Reuters has 20,000 pages of data on financial services, though only four or five pages are used by most. Their value is determined from the total database.

In the industrial economy, excess capacity leads to inefficiency and increases costs. In the intangible economy, it is widespread, functional and inexpensive. It is inexpensive because the key flows are information. Providing additional information flows is different from that of handling physical goods. The long-term trend is for an exponential progression mode and a dramatic fall in unit processing and transmission.

The intangible economy undermines traditional frontiers and distinctions. Sectoral boundaries are crumbling—telecommunications, informatics, electronics are now overlapping. Time-honoured distinctions between work/pleasure, home/workplace, intermediate and financial goods are crumbling.

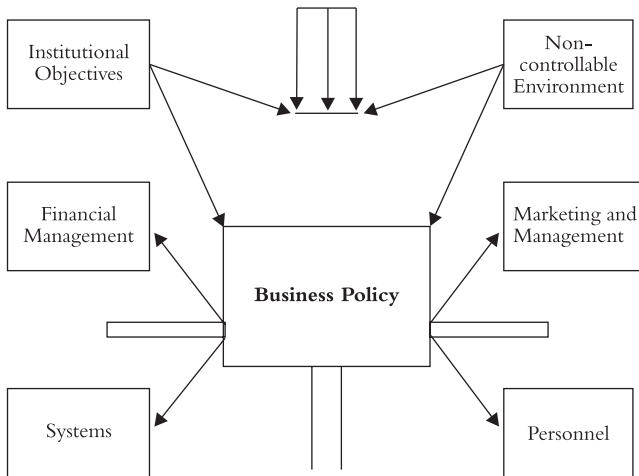
Finally, there is a momentous change in the relationship between suppliers and consumers. The end of information asymmetry has also come about because the customer now knows as much about the products as the supplier.

INTEGRATING MARKETING WITH BUSINESS PLANNING

The traditional marketing approach largely derived its fundamentals from Professor Porter’s (1985) thesis. He argued that for organizations to succeed in a competitive landscape, their strategies must fit their overall organizational objectives. Human resources, IT and finance functions must support the overall organizational strategy to reach the desired objective. Any functional strategy that is inconsistent with this would be doomed to failure. The thesis is far more relevant today than it was earlier.

Banks and financial institutions must make a beginning by involving the marketing departments right from the corporate plans stage to its final execution. It would be difficult to conceive how they could otherwise meet the customer expectations. 'Marketing' departments must be closely integrated with the total working of a financial institution. The old rule that 'make business responsible for marketing and marketing responsible for business', is more relevant than ever before (see Figure 7.2).

Figure 7.2 Marketing Plan in Corporate Plans



Source: Prepared by the author.

Now is the time to get everything inside the company lined up to serve the customers outside your company. The role of marketing is undergoing a change and it is for the top management of financial institutions to ensure that the creative juices flow and the grey cells work in the productive environment. This should not be looked at as a platitudinous objective to be chanted from time to time in customer meets or executive conferences. The organization has to strain every nerve to achieve the given end.

This would necessitate operational efficiency in the organization. A call centre operative who is not trained properly to handle queries, or an email which is not answered in a given timeframe (maximum 4 hours), could mean the loss of a customer. Financial institutions cannot afford to forget that retaining a customer is far more expensive than acquiring a new one. The ultimate aim has to be customer retention and more cost-effective marketing. Instead of advertising to a broad segment of customers, many of whom would not find scattered shot sales pitches interesting, financial

institutions have to target specific customers who are deemed most likely to respond.

Donald Boudreace, Vice Chairman, Chase Manhattan Corporation, is of the view that customization technology is dynamic that is going to work. Thus, excitement must be tempered with a strong dose of reality. It is true that a 'market of one' is now within reach. Financial institutions can engage in electronic dialogues with online customers and formulate offers. A quick credit check, alerting customers regarding changes in interest or proposals to refinance when mortgage rates come down, are some of the ways in which a beginning could be made. These should not be left to marketing departments. In a 'brick and click' model, a very systematic approach has to be adopted. For a detailed analysis of the model see Joshi and Joshi (2009).

MARKETING OBJECTIVES

This is an obvious starting point for marketing policy. A new critical dimension, viz. need for 'retaining' the customers has already been discussed. Along with this, the other objectives are, of course, as relevant as before.

- Profitability.
- Providing high return on investment.
- Achieving certain market share/growth.
- Development of an image.

To this list has to be added a new dimension—customization technology and information infrastructure backed up by marketing strategy behind it. The challenge lies in delivering a customized message; something distinctive and compelling to offer to individual customers. The 'message' and not the medium would count.

Customization has to be viewed broadly. It has to be reviewed as one vital element in an overall customer value proposition and therefore, likely to meet with success. Obviously, such services have to be part of a package that includes other functionalities such as online alerts, easy access and personalization of web pages tailored to meet personal interests. These are some of the ways in which customization would be appreciated.

Decisions regarding marketing are usually taken on an ad hoc basis, for example, the launch of a credit card at a musical evening organized by a financial institute. It is preferable that such events are part of an overall plan.

Although this may be obvious to the marketing personnel, in the hierarchical structure prevailing in the financial institutes, one finds that objective analysis gives way to personal whims and fancies. In the cocoon of regulated environment, banks did not have to work too hard. The pressure to stand out is now growing and the turf is likely to be constantly under attack. There is a marked shift in emphasis. It is now individualized service that will matter. Such initiatives are helped by enormously expensive data warehouse initiatives.

Banks and financial institutions, which have taken initiatives in building robust customer information systems, may not find it difficult to build on them with the help of new technology. For example, after successfully tracking the book-buying habits of its customers, Amazon.com recommends other books that might be of interest to them. Financial institutions must follow the same model. Information collection has to be carried out on a continuous basis. Every click made by a customer either adds information or strengthens what is already available. A second or third visit might warrant a phone call and even a meeting with the customer.

Allowing customers to organize their web pages could allow financial institutions to reach out to the customers in a more personalized way. The results will start showing when financial institutions use the medium's interactivity, immediacy and automation capabilities to add value to their customer relationship.

Online surveys provide immediate feedback, but might annoy customers if they bear too much resemblance to the despised internet spam. The key in most cases is to weave queries into ordinary interactions between customers and the institution, so that feedback can be obtained with a minimum of distraction. Customers do not want to be bothered; therefore, contacts with them have to be better leveraged. Additionally, feedback is important when the matter is fresh in the customer's mind.

There is considerable scepticism with which these views are regarded. Nobody thinks that the Amazon.com model could ever serve a banker or broker. Thus, the idea of a bank suggesting a financial product by looking at a customer's profile is scoffed at. Further, it is also pointed out that barely 2 per cent of the web visitors can be converted into buyers—despite energies spent on simplifying navigation, accelerating the checkout, reducing initial buying risk and enhancing loyalty with incentives, many customers just kick the tires and leave.

This sort of criticism only strengthens the belief that banks and financial institutions need to redouble their efforts and ensure top-quality execution. The distinction between customers' planning their purchases through basic 'research' and their being guided to do so, cannot be glossed over. There

is no rush to offer new products as the customer is probably looking for a calculator or aggregated information regarding a product.

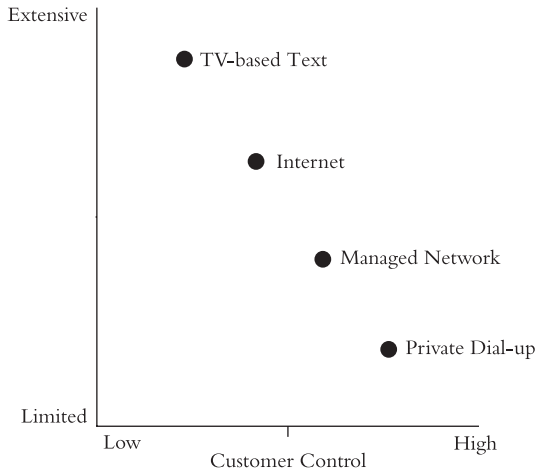
It is now necessary to critically review the changing customer profile—skilled or otherwise. Nowadays, consumers can change their banks at the press of a button from the comfort of their homes. They have access to aggregator websites, which facilitate a comparison of terms and conditions. Further, new players like telecom companies are waiting in the wings with product offerings. Financial institutions would be committing *hara-kiri* if they rely on customer inertia, rather than allowing loyalty to stem from product features and excellence of service.

Here, it would be necessary to briefly make a detour and find out reasons for the customer resistance to making the change. The adoption of the internet for online banking has been hampered by concerns over security and the speed of access. New users of the internet have difficulty in navigating their way to the page that they want. Banks are not making any special efforts to attract customers to the internet facility.

There is a certain trade-off between the advantage of each system from the consumer's point of view and the point of view of the financial institutions. Consumers are concerned with the speed of access, reliability, security and user interface. These in a sense reflect the control customers have as managed networks, dial-up systems are what the customers prefer to have.

Although suppliers are concerned with these issues, there is the additional problem of how to reach a large number of potential customers. The broadcast medium offers a mass marketing reach, while a managed network can afford only a limited reach. The only logical solution would be to use multiple solutions. Figure 7.3 is a diagrammatic representation of the trade-off.

Financial institutions need to watch technological developments very carefully to see how the twin requirements of mass reach and security can be enmeshed. The other factor, which could tilt the scale from private to open networks, would be the need for different 'products' to be available. Additional services would also be in demand. The challenges before brick and click institutions emerging from 'costing' of services are going to be a major strategic problem. The 'marginal costs' of internet services are far too low to warrant comparison with similar services offered at the branches. Branch closures and staff retrenchment could help in reducing overall costs, but despite these measures, they will not reduce 'transaction' costs. The service charges currently levied appear to be arbitrary and at no time does one get satisfactory explanation for the charges from the branch staff.

Figure 7.3 Supplier Reach

Source: Prepared by the author.

The charges for an ATM transaction could be a few paise, while the same transaction at the branch premises could be several rupees. In one case customer would expect to receive benefits for the low cost of operations, while in the other customers will have to pay a hefty price for having the luxury of human interface. The hybrid marketing that would have to be resorted to can be demotivating for high service/high cost channels.

The need of the hour is for a channel for independent products and solutions. This would allow operations and systems complexity costs to be kept to a minimum. The same products can be offered through different channels to target different segments. Their need in terms of guidance, advice and support could be substantial. Those who do not need such support ought to be persuaded to move to a low-cost channel.

Future products will have to be distributed through multiple channels. It is necessary to stress once again that lower transaction cost will result in cost savings, if transactions can be migrated from higher cost services channels in such a way that it allows for cost reduction. Needless to say, the development setup and marketing costs must be under check. Rhetorical questions like, 'Do ATMs make money?' may win points in debates but do not lend strength to the balance sheet.

Customers who use mobile phones, however, are in the habit of paying charges for the services required and used. Thus there is a hope that they may not hold a grudge against such charges.

Another aspect that needs to be briefly discussed is at the branch level, that there is a direct contact and interaction between the bank manager and the customer.

But on the Internet, intermediaries are inevitable between the financial institution and the customer. Bank managements and the branch staff must realize that customers expect different things from electronic delivery of financial services. Customers want information, want to shop around, compare rates and obtain cheaper delivery. Banks want information on customer needs to increase their knowledge about relationships and increase their cross-sell ratios. The result could be a loss of proprietary delivery channels. Financial institutions and banks would soon have to develop intranets to shift information. They must see that corporate information stored individually is transferred to a central place.

The scope for intermediaries to come between the bank and the customer is indeed a cause of concern. We have already seen how aggregator gains access to websites by using customers' identification numbers. Some managers are confident that developing suitable alliances could solve the problem. If banks could form alliances with super markets and airlines, why could they not do so with others? One really needs to be on the lookout for opportunities.

For banks which are yet to get in to e-banking, it is suggested that a very high commitment at top management level is necessary before a coherent online strategy emerges. Following the 'max-e-marketing in the Net Future' the adoption of their following seven max-e-imperatives is suggested:

- Use what you know to drive what you do. Make everything you do to add to what you know. The most significant asset is the behavioural information gained through interaction with customers. The line between success and failure would depend on what you know, how you are organized to use it and to add more of what you need to know.
- Erase the line between product and service. In the net future, financial institutions need to create tightly linked 'offerings' without any separation. In a commoditized market place, such offerings would differentiate your selling ideas.
- Make each relationship as different as each customer. The integration of sales, service and customer care applications from the e-business world with traditional CRM processes can make each customer relationship different.

- Do as little as possible yourself. Outsourcing of activities would be an important ingredient of success.
- Interactive processes should become the products—‘The process is the message.’
- Factor future value into every move. Make the brand experience exceed the brand perception.
- Direct interaction with the user becomes the prevailing way of doing business. Today’s brand experience will determine tomorrow’s ranking. What you do to, for and with the customer that exceeds the brand perceptions builds brand equity and the future value of the relationship.
- Make business responsible for marketing and marketing responsible for business.

Marketing departments in financial institutions are all too familiar with the four Ps (product, price, promotion and place). No doubt these are basic considerations. To these can be added the other important elements, which are:

- Addressability—How does one identify such customers?
- Accountability—How easy is it to reach results?
- Affordability—How easy is it to interact with the customer?
- Accessibility—Are your customers ready, willing and able to receive your message?

Going in the reverse order, banks not only need to undertake surveys of customer needs, but also undertake a massive programme for customer education. Second, unless decisions are backed by data and findings, it would be futile merely to launch products because others are doing it. Thus, unless your customers genuinely need it, it is not advisable to enter into e-financial services. A check list for managers/staff members has been discussed in the next section.

MANAGERS’ CHECK LIST

Banks and financial institutions are not yet reconciled to the idea that customers no longer have the loyalty as was expected in the past. This is because:

- Customers are more sophisticated and price conscious. Further, they prefer to make more informed decisions by comparing the available products.
- Customer groups are changing because of longer life span and urbanization.
- A more consultative relationship is expected. Technically savvy customers are bound to demand:
 - consistent and dependable performance;
 - professionalism, skills and standards of performance;
 - timeliness of service;
 - cordiality and honesty;
 - polite behaviour;
 - safety, security and confidentiality of staff and
 - effective and polite communication.

Thus, customers might shift from one financial institution to another due to a failure of any one of those factors listed above.

EVALUATION OF STRATEGIES

This section discusses the marketing strategy evaluation. The results of any marketing plan must be reflected in the balance sheet and the profit and loss account. One need not wait till the information becomes available at the end of a year or in an unaudited form every quarter. Attainment of specific results is necessary to evaluate a given activity. There is a tendency to substitute sincerity of efforts with results. Sincerity cannot be an excuse for not achieving results.

Some departments function under a mistaken notion that they are not amenable to objective evaluation or audit. It is essential to dispel such a notion and subject 'marketing' to a critical scrutiny not merely from an audit trail creation and adherence point of view but also from the following ones:

- Level of resources allotted. In case of Net marketing they could be a huge amount. For example, some British banks had to spend sums varying from £145 million to £200 million on advertisement; and a further £25 million to create awareness;
- Tactics and strategies used and
- Effectiveness and liaison with other departments.

Under such circumstances, it would be futile to be under the notion that these departments deal with 'intangibles' that are not amenable to evaluation.

At this stage, it is necessary to refer to current research on marketing architecture and its impact on 'marketing', which have been briefly touched on earlier. Marketing executives and top managements must now ensure that they are attuned to perceive changes in these vital fields. Concepts such as 'exchanges', as pointed out earlier, are assuming altogether new dimensions and do not mean what they used to stand for. In fact, marketing and support departments will have to focus significantly on increasing the productivity of their departments. Companies, which have successfully implemented CRM solutions, do report significant operational improvements, including revenue increases per person. Technology has to be leveraged to optimize sales.

GRIEVANCE REDRESSAL

In today's systems, the redressal of simple complaints like an error in a statement, an unaccountable change in balance, regular installment or standing instructions being missed result in complicated messages, mails and irritating conversations.

In times to come, call centres would try and sort it out. Before the customer presses the button, technology would allow agents to retrieve all records instantaneously in screen-pops instead of submitting written requests and waiting for weeks for all the documents to be assembled. Integrated data warehousing, telephony and workflow technology should make this possible in a new and wired world.

MARKET TURBULENCE

Customers need a human touch whenever markets are turbulent. The multi-channel strategy that has been advocated, would stand the financial institutions in good stead.

In conclusion, it can be said that 'e-CRM' would enable the banks and financial institutions to go to the heart of their customers' needs. These could help them to nurture loyal relationships, understand which customers and channels offer the greatest revenue potential and to cross-sell products more efficiently. It is the duty of these financial institutions to ensure that the relationships do not get completely depersonalized.

The main reason why these simple ideas are not translated into action seems to be that banks have not clearly entrusted the work to the branches. In a brick and click model the migration of customers to the internet has to be undertaken by the branches. In fact, it has to be a profit centre activity for them. Swedish banks have very successfully implemented such schemes and the results are very satisfactory.

The second difficulty is that banks are offering their customers more channels of communication, but very little choice. These channels, particularly after the inroads that mobiles have made, need to be well integrated. In this connection, a discussion on the way this problem was tackled by Cisco and Paribas is important. It also throws light on the way internet facilities can be put to use to develop effective customer relationship.

Cisco helped Paribas understand the business impact of the convergence of internet routing and telephony on our multi-channel model. Their team shared with them how Cisco had rethought their mission to integrate convergence into the enterprise. The initial work related to improving the call services (20 million calls a year). The click element did not have to wait long. The bank chose a high-level multimedia platform for real-time sharing. The next task was to improve the work stations. It opted to build a best-of-breed solution. With back-office updates underway the bank could launch its portal. With a single customer identification number to facilitate the migration, it became possible to share information regarding contents, fixing appointments, and so on. Real-time tracing of events and customer file management were enhanced by an event and contact database that recorded interactions across the channels.

The magnitude of the task can be understood when we note that this meant integrating the database of 6 million customers, with daily reporting of events and updating of profiles. This integration now has made it possible for the sales force to log in reminders of future intentions and make contacts positively at the right time. The bank is also able to develop a customer satisfaction scoring card. An electronic platform for bond dealing was the next to follow. Large bond dealing now gets done on the internet. BNP Paribas has rightly claimed that the integrated multi-channel framework has enabled them to manage almost 300 million contacts with their customers, who chose their preferred channel for interactions with the bank.

The next obvious question relates to business results. Customers have seen a sharp all round improvement in service. Each month telephone counters handle more than 2 million calls. Further planning for the sales team has become much easier. The customer relations service centre now plays a more proactive role. Client files are enriched and branch advisers are much

better placed in handling matters. However, the most significant result is the realization by branch staff of their new proactive responsibilities for maintaining contact opportunities generated by the system. As managers embrace this focus customer satisfaction is becoming the key performance metric. Equally important is the fourfold growth in offering credit based solutions to blue-chip clients in 21 countries.

The way ahead is known. It is for banks to ensure that the new mobile penetration, on an almost unprecedented scale, is taken advantage of. Banks and finance companies would lose out if they fail to realize the long-term growth prospects.

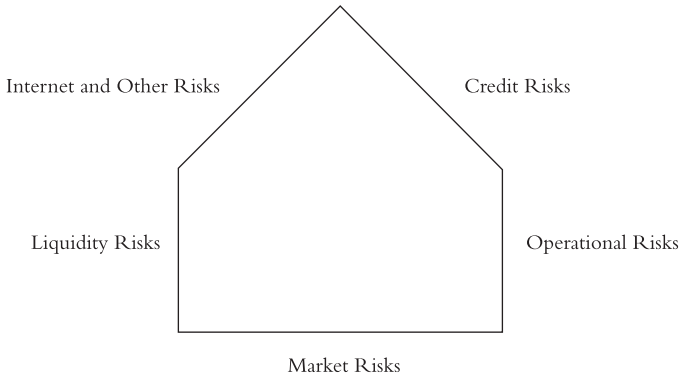
General Aspects of Risk Management

Risk is the probability or likelihood of injury, damage or loss in some specific environment and over some stated period of time. It involves two elements:

- Probability.
- Loss amount.

Risks arise on account of a number of factors. Figure 8.1 indicates very broadly the various factors that have to be taken into account while dealing with risk management. It indicates the factors that impinge on risk assessment and consequently on management; the task of risk management is highly complex and equally demanding. It also provides a brief representation of the most common risks encountered by any financial institution. The list is by no means complete. It is only indicative.

It would be pertinent to mention that a failure in one area could lead to other risks also. An increase in non-performing assets could bring in other risks also. Perhaps, the hexagonal representation gives a better idea about the interconnectivity of risks. For a more detailed review of risk assessment, techniques and their management refer to *Managing Indian Banks* (Joshi and Joshi 2009). Additionally, one has also to look at the risks undertaken by banks on the investments made. We have dealt with these aspects, including the Value at Risk Approach, in *Managing Indian Banks*. The treatment was somewhat elementary as we had noticed that even these introductory aspects were found to be somewhat difficult by a number of participants/readers at seminars who probably had not dealt with these areas.

Figure 8.1 Interrelations of Risks

At this stage it is, absolutely necessary to highlight a very important aspect which has now occupied centre stage and is currently being examined by various authorities, academicians and regulators. The broad range of policy changes could be discerned by a brief look at the recommendations made by Lord Turner (2009) in his review paper submitted to the Chancellor of the Exchequer. Some of these aspects have been discussed in the chapter on regulation. Suffice it to say that at this point in time these are mere suggestions and it would be quite some time before they are implemented globally.

- The quality and quantity of overall capital in the global banking system should be increased so that this results in minimum regulatory requirements, significantly above existing Basel rules.
- The transition to future rules should be carefully phased given the importance of maintaining bank lending in the current macroeconomic climate.
- Capital required against trading book activities should be increased significantly (for example, several times) and a fundamental review of the market risk capital regime (for example, reliance on VAR measures for regulatory purposes) should be launched.
- Regulators should take immediate action to ensure that the implementation of the current Basel II capital regime does not create unnecessary procyclicality. This can be achieved by using 'through the cycle' rather than 'point in time' measures of probabilities of default.

- A counter-cyclical capital adequacy regime should be introduced, with capital buffers, which increases in economic upswings and decreases in recessions.
- Published accounts should also include buffers, which anticipate potential future losses, through, for instance, the creation of an 'Economic Cycle Reserve'.
- A maximum gross leverage ratio should be introduced as a backstop discipline against excessive growth in absolute balance sheet size.
- Liquidity regulation and supervision should be recognized as of equal importance to capital regulation.
 - More intense and dedicated supervision of individual banks' liquidity positions should be introduced, including the use of stress tests defined by regulators and covering system-wide risks.
 - Introduction of a 'core funding ratio' to ensure sustainable funding of balance sheet growth should be considered.

INSTITUTIONAL AND GEOGRAPHIC COVERAGE OF REGULATION

- Regulatory and supervisory coverage should follow the principle of economic substance not legal form.
- Authorities should have the power to gather information on all significant unregulated financial institutions (for example, hedge funds) to allow assessment of overall system-wide risks. Regulators should have the power to extend prudential regulation of capital and liquidity or impose other restrictions if any institution or group of institutions develops bank-like features that threaten financial stability and/or, otherwise, become systemically significant.
- Offshore financial centres should be covered by global agreements on regulatory standards.

It is absolutely clear that the whole gamut of financial institutions' working is under critical evaluation. However the limited aspects pertaining to internet security are a matter of concern and in this chapter the discussion would merely touch on the broader questions. Basically, the questions pertain to the assumptions on which the predictive models were based and their limitations. There was a time when these models were recommended for adoption by various regulators, including the RBI and what we are now witnessing is a retreat from the so-called 'market would

take care' approach. It is true that some of the fault lies with the way these models were used to derive conclusions. It would not be wrong to say that lust for profits and bonuses (a part of remuneration policy) did lead to a gross misuse of these techniques for prediction. It needs to be emphasized that the conclusions have to be tempered with experience (grey hair has a unique place in financial institutions) and reviews at appropriate levels.

However, part of the blame lies with the regulators. Institutions like the IMF and the World Bank put too much faith in the market mechanism and encouraged similar fundamentalist policies for adoption which, but for such dogmatic beliefs, could not have been easily adopted.

This chapter focusses on nature of additional risks faced by banks/financial institutions when they are using online channels. The banks, brokers or financial institutions need to take note of all the aspects mentioned earlier and in addition to that deal with risks specific to the relevant aspects of an electronic environment, which would include transaction speed, geographic reach and user anonymity. One of the major problems is to integrate the newer techniques with legacy systems. It is necessary to emphasize that risk management is an ongoing process of identifying, measuring, monitoring and managing all significant operational, legal and reputation risks.

It has been noticed that many institutions are somewhat indifferent to the aspects of internet risk management and look on these aspects as part apart. These are not yet an integral part of activities. Therefore, we need to start the discussion from the basic requirements of any such programme. A good starting point is to look at the measures suggested by the Federal Deposit Insurance Corporation (FDIC) in USA.

Following the FDIC guidelines, these areas can be divided into the following broad areas:

- General areas: Planning, policies and procedures. Distribution of duties, accountability and delegation of authorities, regulatory compliance and audits, and so on.
- Transaction processing: User authentication, information integrity, and non-repudiation of transactions and data confidentiality.
- Systems administration: Resource requirements, system security, contingency planning, outsourcing policies, and so on.

The results of this process need to be integrated into the following:

- Strategic planning and feasibility analysis.
- Management supervision and control.
- Operating policies and procedures.

94 E-finance

- System audit, administration and testing.
- Physical and transaction system security.
- Incident response and preparedness plans.

These techniques are also applicable to traditional risk management methods. Risks peculiar to the electronic systems must now be considered because these areas are the ones, which would be areas of concern for the regulators. Financial institutions would henceforth be evaluated, not only in terms of their 'Risk Management Systems', but probably on a much wider scale as highlighted by Turner (2009). It is, no doubt, in the institution's own interest to have systems which would safeguard its own and the interests of its customers.

ELECTRONIC SYSTEM RISKS

Conceptually, these risks can be broadly classified into two broad groups. There are risks, which can lead to disabling the system from functioning properly. The other group includes risks relating to data tampering and misuse. In the first category hacking can be included, which is done either to show off one's technical abilities (ethical hackers in the age group of 15–18) or with malicious intent (carried out by 'black' hackers).

The other area pertains to fraudulent data misuse in order to have access to sensitive information for some personal gain. It is worth noting that in 70 per cent of the cases it is the staff, which is found to have been responsible for the mischief. Chapter 11 deals with network security in greater detail. Authors like Ankit Fadia or Yogesh Barua and Prateek Dayal have explored these areas thoroughly and both the technical and non-technical readers would find these of great use (see Barua 2005, Dayal 2008, Fadia 2009). It must be pointed out, however, that there are bound to be technological advances and today's methods could be quite outmoded tomorrow. Thieves try to be two jumps ahead of the authorities.

A review of data protection techniques is discussed in the next section. The material has been largely drawn from FDIC circulars and those issued by other regulatory bodies.

PREVENTIVE MEASURES

Preventive measures include sound security policies, well-designed system architecture and properly configured firewalls. Additionally, two more

measures viz. assessment tools and penetration analysis are also discussed. Some of these aspects have been discussed in the chapter on regulation as well. At this point in time these are mere suggestions but they may be implemented at a later date.

Vulnerability assessment tools generally involve running scans on a system to proactively find out vulnerabilities, flaws and bugs in software and hardware. These tools can also detect the loopholes that allow unauthorized access to a network or insiders to misuse the system. Penetration analysis involves an independent party (internal or external) testing an institution's information system security to identify (and possibly exploit) vulnerabilities in the system and surrounding processes. Using vulnerability assessment and performing regular penetration analyses will assist an institution in determining what security weaknesses exist in its information systems. Detection measures involve analyzing available information to determine if an information system has been compromised, misused or accessed by unauthorized individuals. Detection measures may be enhanced by the use of intrusion detection systems (IDSs) that act as a burglar alarm, alerting the banker, service provider to potential external break-ins or internal misuse of the system(s) being monitored. Another key area involves preparing a response programme to handle suspected intrusions and system misuse once they are detected. Institutions should have an effective incident response programme outline in a security policy that prioritizes incidents, discusses appropriate responses to incidents and establishes reporting requirements. Before implementing some or all of these measures, an institution should perform an information security risk assessment. Depending on the risk assessment, certain risk assessment tools and practices discussed in this section may be appropriate. However, use of these measures should not result in decreased emphasis on information security or the need for human expertise.

RISK ASSESSMENT/MANAGEMENT

A thorough and proactive risk assessment is the first step in establishing a sound security programme. This is the ongoing process of evaluating threats and vulnerabilities, and establishing an appropriate risk management programme to mitigate potential monetary losses and harm to an institution's reputation. Threats have the potential to harm an institution, while vulnerabilities are weaknesses that can be exploited. The extent of the information security programme should be commensurate with the degree of risk associated with the institution's systems, networks and information

assets. For example, compared to an information-only website, institutions offering transactional internet-banking activities are exposed to greater risks. Further, real-time funds transfers generally pose greater risks than delayed or batch-processed transactions because the items are processed immediately. The extent to which an institution contracts with third-party vendors will also affect the nature of the risk assessment programme.

PERFORMING THE RISK ASSESSMENT AND DETERMINING VULNERABILITIES

Performing a sound risk assessment is critical to establishing an effective information security programme. The risk assessment provides a framework for establishing policy guidelines and identifying the risk assessment tools and practices that may be appropriate for an institution. Institutions still should have a written information security policy, sound security policy guidelines and well-designed system architecture, as well as provide for physical security, employee education and testing, as part of an effective programme. When institutions contract with third-party providers for information system services, they should have a sound oversight programme. At a minimum, the security-related clauses of a written contract should define the responsibilities of both parties with respect to data confidentiality, system security and notification procedures in the event of data or system compromise. The institution needs to conduct a sufficient analysis of the provider's security programme, including how the provider uses available risk assessment tools and practices. Institutions also should obtain copies of independent penetration tests run against the provider's system.

When assessing information security products, management should be aware that many products offer a combination of risk assessment features, and can cover single or multiple operating systems. Several organizations provide independent assessments and certifications of the adequacy of computer security products (for example, firewalls). While the underlying product may be certified, banks should realize that the manner, in which the products are configured and ultimately used, is an integral part of the products' effectiveness. In relying on the certification, banks should understand the certification process used by the organization certifying the security product. Other examples of items to consider in the risk assessment process include identifying mission-critical information systems and determining the effectiveness of current information security programmes. For example, a vulnerability might involve critical systems that are not

reasonably isolated from the internet and external access via a modem. Having up-to-date inventory listings of hardware and software, as well as system topologies, is important in this process. Assessing the importance and sensitivity of information, and the likelihood of outside break-ins (for example, by hackers) and insider misuse of information, is equally important. For example, if a large depositor list is made public, that disclosure can expose the bank to reputation risk and the potential loss of deposits. Further, the institution can be harmed if human resource data (like salaries and personnel files) are made public. The assessment should identify systems that allow the transfer of funds, other assets or sensitive data/confidential information, and review the appropriateness of access controls and other security policy settings. Assessing the risks posed by electronic connections with business partners has to be an integral part of such an exercise. The other entity may have poor access controls that could potentially lead to an indirect compromise of the bank's system. Another example involves vendors that may be allowed to access the bank's system without proper security safeguards, such as firewalls. This could result in open access to critical information that the vendor may have 'no need to know'. Determining legal implications and contingent liability concerns associated with any of the aforementioned scenarios is also necessary. For example, if hackers successfully access a bank's system and use it to subsequently attack others, the bank may be liable for damages incurred by the party that is attacked.

POTENTIAL THREATS TO CONSIDER

Serious hackers, interested computer novices, dishonest vendors or competitors, disgruntled current or former employees, organized criminals, or even agents of espionage pose a potential threat to an institution's computer security. The internet provides a wealth of information to banks and hackers alike on known security flaws in hardware and software. Using almost any search engine, average internet users can quickly find information describing how to break into various systems by exploiting known security flaws and software bugs. Hackers also may breach security by misusing vulnerability assessment tools to probe network systems, then exploiting any identified weaknesses to gain unauthorized access to a system. Internal misuse of information systems remains an ever-present security threat. Many break-ins or insider misuses of information occur due to poor security programmes. Hackers often exploit well-known weaknesses and security defects in operating systems that have not been appropriately addressed by

the institution. Inadequate maintenance and improper system design may also allow hackers to exploit a security system. New security risks arise from evolving attack methods or newly detected holes and bugs in existing software and hardware. Also, new risks may be introduced as systems are altered or upgraded, or through the improper set-up of available security-related tools. An institution needs to stay abreast of new security threats and vulnerabilities. It is equally important to keep abreast of the latest security patches and version upgrades that are available to fix security flaws and bugs. Information security and relevant vendor websites contain much of this information. Systems can be vulnerable to a variety of threats, including the misuse or theft of passwords. Hackers may use password-cracking programmes to decode poorly selected passwords. The passwords may then be used to access other parts of the system. By monitoring network traffic, unauthorized users can easily steal unencrypted passwords. The theft of passwords is more difficult if they are encrypted. Employees or hackers may also attempt to compromise system administrator access (root access), tamper with critical files, read confidential email or initiate unauthorized emails or transactions. Hackers may also use 'social engineering', a scheme using social technique to obtain technical information required to access a system. A hacker may claim to be someone authorized to access the system, such as an employee or a certain vendor or contractor. The hacker may then attempt to get a real employee to reveal user names or passwords, or even create new computer accounts. Another threat involves the practice of 'wardialing', in which hackers use a programme that automatically dials telephone numbers and searches for modem lines that bypass network firewalls and other security measures. A few other common forms of system attack include denial of service (system failure), which is any action preventing a system from operating as intended. It may be the unauthorized destruction, modification or delay of service. For example, in a 'SYN Flood' attack, a system can be flooded with requests to establish a connection, leaving the system with more open connections than it can support. Thus, legitimate users of the system being attacked are not allowed to connect until the open connections are closed or can time out. Internet Protocol (IP) spoofing allows an intruder via the internet to effectively impersonate a local system's IP address in an attempt to gain access to that system. If other local systems perform session authentication based on a connection's IP address, those systems may misinterpret incoming connections from the intruder as originating from a local trusted host and not require a password.

Trojan horses are programmes that contain additional (hidden) functions that usually allow malicious or unintended activities. A Trojan horse

programme generally performs unintended functions that may include replacing programmes, or collecting, falsifying and destroying data. Trojan horses can be attached to emails and may create a 'back door' that allows unrestricted access to a system. The programmes may automatically exclude logging and other information that would allow the intruder to be traced. Viruses are computer programmes that may be embedded in other code and can be self-replicated. Once active, they may take unwanted and unexpected actions that can result in either nondestructive or destructive outcomes in the host computer programmes. The virus programme may also move into multiple platforms, data files or devices on a system and spread through multiple systems in a network. Virus programmes may be contained in an email attachment and become active when the attachment is opened.

BIS had drawn out a set of 14 principles for a proper development of a mechanism for risk management. It is necessary to say that prescribing principles should not turn out to be counter productive. Each bank's risk profile is different and requires a tailored approach for risk mitigating efforts appropriate for the scale of e-banking operations, the materiality of risks present and the institute's willingness and ability to manage the risks. This does imply that 'one-size fits all' approach to e-banking risk management may not be appropriate. It would be useful to bring out the guidelines brought out by BIS and also by FDIC for the use of bank examiners.

A combination of prescriptive measures suggested by the BIS and examination techniques proposed by FDIC are a good starting point. There is considerable unanimity about the proposals made and one is on a safe wicket in adopting them.

The existing risk-management principles must be tailored, adapted and in some cases extended to address specific risk management challenges created by the peculiar characteristics of e-banking activities. The RBI can extend the policies enunciated in 1998 (RBI Circulars dealing with Asset/Liability Management and Risk Management: (a) DBOD no. BP.BC.94/21.04.098/98 and (b) DBOD no. BPsc.BC.98/21.04.103/99) and make it mandatory for banks broadly to adopt the suggestions made by BIS in its report on 'Risk Management Principles for Electronic Banking' in consultation with RBI. BIS is quite right in asserting that setting detailed risk management requirements must not be counter productive. Each bank's risk profile is different and requires a tailored approach for risk mitigation appropriate for the scale of e-banking operations, the materiality of risks present and the institute's willingness and ability to manage the risks. This does imply that one-size fits all approach to e-banking risk management may not be quite suited.

Broadly, the risk management efforts fall into three groups.

MANAGEMENT OVERSIGHT

Effective management oversight of the risks associated with e-banking needs to be in place and risk management should be integrated with overall risk management. There must be an explicit, informed and documented strategic decision, covering specific accountabilities, policies and controls, to address risks. Key aspects of security control process must be covered.

DUE DILIGENCE

This includes comprehensive due diligence and management oversight processes for outsourcing relations and third party dependencies.

SECURITY CONTROLS

This includes:

- Authentication of e-banking customers.
- Non-repudiation and accountability for e-banking transactions.
- Appropriate measures for segregation of duties.
- Data integrity of e-banking transactions, records and information.
- Establishment of clear audit trails for e-banking transactions.
- Confidentiality of key banking transactions.
- Legal and reputational risk management principles.
- Appropriate disclosures for e-banking services.
- Privacy of customer information.
- Capacity and business continuity.
- Contingency planning to ensure availability of e-banking services.
- Incident response planning.

Against the backdrop of preceding information, the Basel Committee on Risks for Electronic Banking has developed the following 14 key risk management principles:

- Management of outsourcing and third party dependencies.
- Segregation of duties.

- Proper authorization measures and controls.
- Clear audit trails.
- Authentication of all entities, counterparts and data.
- Non-repudiation of e-banking transactions.
- Comprehensive security.
- Integrity of banking transactions, records and information.
- Appropriate disclosure for e-banking services.
- Confidentiality and privacy of customer information.
- Business continuity and contingency planning.
- Incident response planning.
- Role of supervisors.

These suggestions need to be supplemented with a report prepared by FDIC for bank examiners. The summarized version is in two parts. The standards represent performance objectives to ensure that bank operates in a safe and sound manner and that the bank's objectives are carried out. Associated risks represent potential threats because of failure to adhere to such standards.

There are problems associated with other e-finance activities like broking, alternate systems of trading, foreign exchange transactions, and so on. These would be taken up in the chapter on regulation.

It is important for financial institutions to develop and implement appropriate information security programmes. Whether systems are maintained in-house or by third-part vendors, appropriate security controls and risk management techniques must be employed. A security programme includes effective security policies and system architecture, which may be supported by the risk assessment tools and practices discussed earlier. Information security threats and vulnerabilities, as well as their countermeasures, will continue to evolve. As such institutions should have a proactive risk assessment process that identifies emerging threats and vulnerabilities to information systems.

A sound information security policy identifies prevention, detection and response measures. Preventive measures may include regularly using vulnerability assessment tools and conducting periodic penetration analyses. Intrusion detection tools can be effective in detecting potential intrusions or system misuse. Institutions should also develop a response programme to effectively handle any information security breaches that may occur.

It would be important to indicate here the part played by technology in the risk management process and the way to select the appropriate system. While selecting the appropriate system it would be useful to:

- Establish clear goals for the risk management system.
- Identify each operation's needs.
- Survey available technology.
- Never trust a demo model.
- Take everything with a pinch of salt.

It would at this stage be useful to highlight the relationship between key business risks and activities undertaken.

- Poor loan quality credit risk.
- High funding costs interest risk.
- Asset/liability management, yield curve/cash-flow risks.
- Poor controls operational risks.
- Frauds legal/reputational risks.

The term technology refers to two distinct aspects: (a) The physical components of technology that are required for a risk management system and (b) the software that drives the application. It needs to be mentioned here that after the crisis, serious doubts are raised about the software used and the work done by the rating agencies. It would not be wrong to say that a number of accepted arrangements for risk assessment and management are in the melting pot and it would require a strong regulator and the strong finance ministry to undertake the kind of changes, which are required to be taken on an urgent basis.

OUTSOURCING

Very often organizations outsource e-banking systems and services. Obviously great care has to be exercised in dealing with such system. A brief outline of the practices to be adopted for risk management when such systems are outsourced is given in the next section. This aspect has been dealt with in some detail in the chapter on Network Security. These would have to be borne in mind while dealing with risk management systems.

RISKS BEYOND THE ORGANIZATIONAL CONTROL

The management of risks at the organizational level has been discussed so far in a somewhat abstract way. But there are areas where the organization may suffer losses on account of factors beyond its control. Following is

a case where services required were not available when they were most needed.

Hurricane Ivan illustrated a need for new forms of internet business risk management when it damaged an undersea cable and disconnected the Cayman Islands. The disconnection lasted more than two days and is an example of a risk beyond the control of the enterprise or the telecommunications carrier: a force *majeure* risk, or act of God. No amount of firewalls, intrusion detection or patches would have prevented it. Another undersea cable running to the Cayman Islands might have minimized the downtime, but at some point, the expense becomes greater than the risk or at least greater than the cost of insurance for the risk.

On the internet, physical risks such as hurricanes, floods and earthquakes are not the only force *majeure* risks, and not the most economically significant ones. Hurricanes are constrained in geographical scope. Worms, denial-of-service attacks and terrorism are not so constrained, and could cause even more aggregate damage than a hurricane. Put another way, offshore content caching may help prevent an outage due to a hurricane, but will not necessarily avoid a worm.

To conclude it can be said that organizations must be proactive, read the signs on the wall and start initiating steps which the current crisis demands. Only then would it be possible to restore the confidence.

Risk Management for E-banking and E-insurance

Chapter 8 discussed and examined some of the general tools for assessment and management of risks on the internet. This chapter specifically considers insurance and banking industries' attempts at controlling and managing these risks. In particular, two features will be highlighted. These industry groups are usually reluctant to disclose any intrusions into their systems. This stems from fears about further attacks and about adverse publicity, which could lead to panic reactions amongst clients.

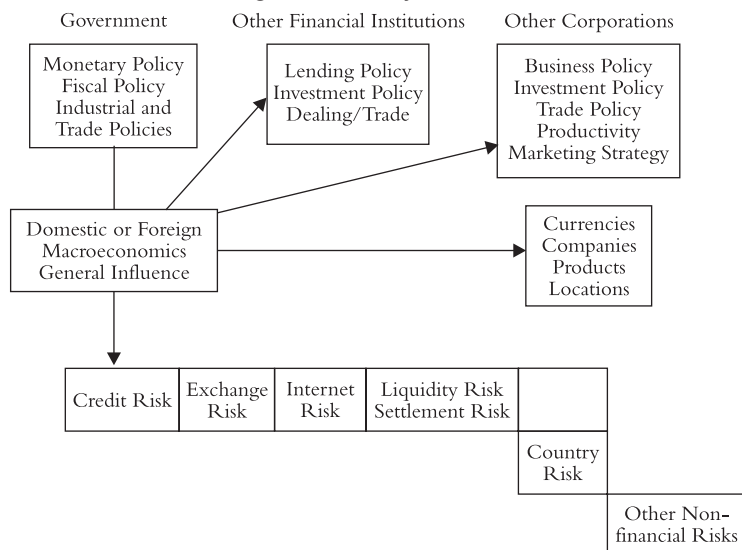
The South-East Asian crisis and the Barings Bank debacle were perhaps the immediate causes for banks and the supervisors to work together to evolve sound policies for this vital area of management for the financial services industry. It is indeed heartening that the problem is being analysed globally and that most countries are not only examining these issues, but are also concerned with developing appropriate strategies suited to their conditions. A particularly encouraging feature is that whenever there are differences of views amongst central regulators, they are aired and even made available on their websites for comments. Further, the organizations, which have framed these rules, do not claim that these are 'model' rules and that they need to be copied *in toto*.

Figure 9.1 describes the various forces that have to be taken into consideration.

BIS RECOMMENDATIONS

A summary of recommendations made by Bank for International Settlement (BIS) has been discussed in the following paragraphs. These are part of

Figure 9.1 Analysis of Risk



Source: Prepared by the author.

the total set of recommendations for risk management and need to be viewed in that context. A bank or financial institute developing the e-trade channel must be equally careful about the total apparatus it has for the risk management function. E-banking must be a part of that scheme. Further, organizations like the Federal Deposit Insurance Corporation in the US also provide specific guidelines which organizations could take advantage of.

The recommendations are summarized in the next section. BIS is quite right in asserting that fulfilling detailed risk management requirements must not be counter productive. Each bank's risk profile is different and a tailored approach is required for risk mitigation appropriate for the scale of e-banking operations, the materiality of risks present and the institute's willingness and ability to manage the risks. This does imply that 'one-size fits all approach' to e-banking risk management may not be quite suitable.

As explained in Chapter 8, the risk management efforts broadly fall into three groups:

1. Management Oversight.
2. Due Diligence.
3. Security Controls.

Against the backdrop of the preceding information, the Basel Committee on Risks for Electronic Banking has developed 14 key risk management principles, as elaborated in Chapter 8.

THE INSURANCE SECTOR

Some of the principles enunciated by the International Association of Insurance Supervisors are discussed in this section. Companies must be more conscious of strategic risks associated with an internet strategy. These risks are critical and would be more so when new products designed for sale on the Internet reach the market. The new underwriting opportunities that would become available must be kept in mind. A critical aspect to be examined relates to the risks posed by e-commerce that are new or different in scale or impact from traditional business conducted through other distribution channels. Reputations are at stake as mistakes can multiply and spread quickly.

STRATEGIC RISKS

These risks arise when a company engaging in new business strategy, does not analyse the implications that decision on electronic commerce will have on other parts of the organization or the company as a whole. Without such a plan, the risk of mistakes occurring increases and the chances of the strategy succeeding decrease.

The impact on the solvency should be the overreaching consideration in the analysis. In addition the company should be wary of the following factors:

- The global nature and rapid development and growth of e-commerce will put pressure on its planning and implementation of online operations, in particular, product design and technological applications.
- The Internet is an efficient way of doing business, but it is far from being cost free. System costs and maintaining customer awareness of the website may involve significant advertising costs.
- Brand loyalty may evaporate in the face of competition. Customers could switch their business from one to the other company.

- There is a danger of some customers being neglected. There is an equal danger that research, product innovation, data security and even risk management may be neglected.
- The speed of processing may complicate management of information.
- The dangers of adverse selection could increase and there could be inadequate disclosure by the customers.
- It is the responsibility of the Board to choose strategies that reflect the company's desired risk profile, functional capabilities and solvency. It must decide how its internet strategy will influence the company's philosophy, the way it conducts business and its financial situation.

Without a well thought out strategy, the decision to engage in e-commerce may result in an unwarranted increase in risks at the operational level and an unproductive drain on resources.

OPERATIONAL RISKS

These relate to risks that arise as a result of a failure or default in the IT infrastructure. There could even be deficiencies in the structure available. It may not

- have the capacity to handle increased traffic, process transaction and volume;
- be scalable;
- be accessible all the time due to a lack of fault tolerant technology;
- be secure from internal and external disruption;
- be accessible, compatible or interoperable in every market;
- have appropriate policies and controls in place for third-party vendors; and have adequate scrutiny of the service provider's operational viability, financial liquidity and project management skills.

TRANSACTION RISKS

Transaction risks arise on account of an unauthorized alteration or modification to texts, information or data transmitted over the computer network between an insurer and the client or vice versa. In e-commerce these risks

arise mainly on account of technology. This risk also includes information, which is hosted on the server or website of a 'partner' third party.

DATA SECURITY RISKS

These risks arise due to losses, unintentional changes or leaks of information or data in computer systems. These could be broadly divided into two categories. Incompatibility of the data systems or part of the data system information leaks or information loss may be the cause for such risks. The external links could lead to data breaks. A customer's personal data may be illegally accessed. These could complicate and in some cases, negate the company's ability to authenticate information and data. Information concerning an insurance contract may be changed without authorization after the system has been broken into. Thus, a company's reputation may suffer.

CONNECTIVITY RISKS

Failure in one part of the system may impact all or other parts of the system. If any part of the internet's operational system is damaged as a result of intentional or negligent actions, the company may fail to provide service to clients.

CONDUCT OF BUSINESS RISKS

The laws and regulations are developed with the view that business will be conducted on a person to person basis, with proper documentation. E-commerce poses new issues with attendant risks, such as:

- Authenticating the identity of a customer.
- Verifying and maintaining the security of electronic documents and signatures.
- Notification of contract-related information to safeguard the interests of the client and the company.
- Format and presentations wherein disclosure and disclaimer requirements are met.
- Providing policyholders with a proof acceptable to regulators or other third parties.

- Acceptance of electronic payments in lieu of cheques, drafts or cash.
- Meeting record retention requirements.

Supervisors apprehend that a host of legal issues, including the status of the insurer, the applicable laws, location of the company and, therefore, by whom and how it would be supervised, would sooner or later arise. They are also afraid that the clients may not be aware of all the risks involved and when and if a problem arises it may be too late even for a proper remedy to be found.

ALTERNATE SYSTEMS OF TRADING

The Securities and Exchange Board of India (SEBI) has specifically indicated the use of appropriate technology for risk management. Following is a summary of their major conclusions:

- Exchanges must ensure that brokers have a system-based control on the trading limits of clients, and their exposures. There must be pre-defined limits on the exposure and turnover of each client.
- The systems should be such that client risks could be immediately assessed and that the client would be informed within a reasonable time frame.
- The reports on margin requirements, payment and delivery, should be made known to the client through the system.
- Contract notes must be issued within 24 hours or as per existing rules.
- No cross trades should be undertaken.
- The other rules applicable to brokers should, no doubt, continue to operate.
- Documents should be authenticated through digital signature, electronic certification, and so on.

The following security measures are mandatory for all internet-based trading systems:

- User ID, first-level passwords, automatic expiry of passwords and reinitializing access on entering fresh passwords.
- All transaction logs with proper audit trails and facilities to be maintained.

- Suitable firewalls between trading set-up connected to the exchange system and the internet trading system.
- Secured socket-level security for server access through internet.

The SEBI has gone a step further and recommended the following: (a) microprocessor-based smart cards; (b) dynamic password; (c) 64bit/128 bit encryption and finally (d) second-level password.

Standards for interface between the brokers and clients have also been prescribed. The rules also give detailed instructions to brokers to use the same logic or priorities used by exchanges to treat client orders. Brokers are also to maintain all activities/alerts log with audit trail facility. A unique numbering system, which is internally generated, is also mandatory. There is a considerable overlap of the risk management suggestions of various sectors. Many suggestions by insurance regulators would, therefore, be equally applicable to banking/broking.

CONCLUSION

Many of the requirements can be taken care of by technology. The book refrains from going into these in great details as management would have to take these decisions themselves depending on their specific requirements. Further, the developments are so fast that the suggestions could be outmoded before they are made. While some of the aspects on security are covered in Chapter 8, the details on computer crimes in the next chapter drive home the message for greater attention to risk management.

Cyber Crimes

If cyberspace is a type of community, a giant neighbourhood made up of networked computer users around the world, then it seems natural that many elements of a traditional society can be found taking shape as bits and bytes. With electronic commerce we witness electronic merchants, plugged-in educators and doctors treating patients online. It should not come as a surprise that there are cyber criminals.

As an unregulated medley of corporations, individuals, governments and educational institutions that have agreed to use a standard set of communication protocols, the internet is wide open to exploitation. There are no 'regulators' and this lack of law enforcement leaves net users to regulate each other according to the reigning norms of the moment. Community standards in cyberspace are vastly different from the standards found at the corner of a main street. Cyberspace is a virtual tourist spot where faceless, nameless con artists can work the crowds. The critical issues now facing us can be divided into two broad categories:

- Denial of Service Attacks: The criminal's goal is to cause damage to the system (hacking, cracking and sending malicious code viruses) or computer network.
- The computer is the target of attacks.

At this stage it is important to bring out a major difference in treatment in the first edition of the book and this edition. In the first edition, our endeavour was to show how the Information Technology Act, 2000, had made provisions for various illegal acts and we also described some of

these. We would now go into more specific questions regarding the ways the guilty can be punished and how the aggrieved parties can get redress. Questions of admissibility of evidence and the precautions that bankers should take would be referred to.

At this stage we need to point out that there is a great need for a very vigilant approach in the current phase. In a crisis situation very often guards are lowered and sometimes even routine checks are ignored. A very rigid attitude towards checks needs to be adopted and extra care needs to be taken to ensure that advantage is not taken of by certain rogue elements. Further, we must show that managements of financial institutions (FIS) are vigilant and that excesses of any sort are avoided. Board of Directors and more particularly the Independent Directors must closely watch these aspects and must show zero tolerance towards deviations. Board overview of risk management function is critical and crucial in the current situation.

A criminal act takes place when a particular enactment lays down penalties and offences. In addition to the IT Act, 2000, the Code of Criminal Procedure, The Indian Penal Code, the Evidence Act and the Bankers' Book of Evidence Act have a bearing on cyber crimes.

More than 50 per cent of 100 million computers are networked. One can imagine the magnitude of the challenge of preventing infiltration into computer systems and challenges to computer security and intellectual property.

Computer criminals comprise co-workers, insiders, disgruntled employees or even the lazy ones, competitors, crackers and hackers. Their attacks range from unauthorized access by employees to break-ins by intruders. Before proceeding further, it might be useful to give a brief note on 'Computer speak'.

Term Definitions:

- Hackers: Use illegal methods of accessing a computer.
- Crackers: Programmes to extract information and benefit from it.
- Stealers: Beg, borrow or steal—passwords and other critical information.

Computer crimes take several forms including sabotage, revenge, vandalism, theft, eavesdropping and 'data diddling', credit card frauds, counterfeiting, bank embezzlement and theft of secret documents. Introducing 'worms'/viruses are other forms of computer crimes. The other serious possibilities are information attacks on military, central banks, electricity companies and softwares in use.

Why and how do they occur? The perceived anonymity and the huge financial gain could be the main reasons. Other reasons are as follows:

- Research and development expenses, for a competitor who steals the information, would be nil and would allow the competitor to go ahead in technology.
- Network administrators' laxity.
- Failure to monitor security programmes allows 'hackers' to access the networked system and crimes often go undetected.
- Disgruntled employees or those whose services are terminated could create a security breach.
- Social engineering is used to build a friendship with employees and gain access to information.
- Cryptographic keys can be figured out by timing the computers.
- Firewalls and system probing.
- 'Cracker' programme to identify passwords is used to try every word in the dictionary as a password.
- Network file used to share files between systems is exploited through well-known vulnerabilities.
- 'Sniffing' allows all traffic on a network to be sniffed to collect authorized password.
- Another method of virus infection is transmitted via word files. Word documents are embedded with viruses sent via email. There is no way to see that a document is infected until it is opened.

For the simplicity of analysis one could broadly group these points with reference to certain sections of the IT Act.

- Section 43 (a) lays down that a person who accesses or secures access to such computer system or network would be liable to pay damages by way of compensation not exceeding one crore of rupees to the person so affected.
- Section 43 (b) makes a person liable to pay damages for downloading copies or extract any data or information from such a computer.
- Introduction or causing any computer contaminant or computer virus into any computer system or computer network would be liable for paying damages.
- Causing damage to a computer deliberately.
- Any person who does any or all of the following is liable to be charged for committing a crime:

- Assisting another person to gain unauthorized access.
- Damaging a computer system.
- Manipulating the data for financial benefit.
- Transferring service charges to an account of a person who has not availed the service.

The idea is not to present an exhaustive summary of the provisions of the Act, but to make readers aware of the crimes that can be perpetrated and the penalties that are levied for such criminal acts. A word of caution is absolutely necessary. The broad categories listed previously are further broken down and various details emerge. Inserting a CD or a floppy may not be a criminal activity, but browsing could certainly be one. There are a number of interpretations and elaborations not only of these sections, but also of similar sections in other countries like UK or USA.

At this stage the impact of some of these criminal activities on the working of FIs needs to be examined. The BIS (Bank for International Settlement) in its report on 'Risks management for electronic banking' presents a list of various risks associated with banking activities. Table 10.1 presents a list of these criminal activities.

Table 10.1 Cyber Crimes and Their Effect

<i>Criminal Act</i>	<i>Possible Manifestation</i>	<i>Potential Effect</i>
Unauthorized system access	Hackers enters internal systems; confidential information is intercepted, data gets corrupted; systems crash.	Loss of data, theft of information, costs of repairing perceived insecurity of bank systems.
Employee frauds	Alteration of data in order to draw funds from general bank accounts; theft of smart cards.	Reimbursement customer losses; reconstruction of accurate data; legal or regulatory sanctions.
Counterfeiting of electronic money	Criminals alter or duplicate electronic money to obtain goods or funds.	Liability for falsified money. Replacing costs associated with a compromised system.
Repudiation of a transaction	Transaction completed but customer denies that transaction took place.	Possible loss of funds or legal expenses to prove that transaction was authorized.
Significant breach of security	Introduction of virus; illegal entry by a hacker.	Customers may discontinue the use of that product or service; affected customers may leave and others follow.
Money laundering	Misuse by criminals to engage in money laundering.	Legal sanctions for non-compliance.

Source: Summary of BIS Report on E-finance Risks.

PROBLEMS OF ENFORCEMENT

The first question that comes up relates to admissibility of evidence. With respect to admissibility, the question is whether electronic records are admissible in a court of law. The distinction between 'Real' and 'Hearsay' comes into play. Real evidence is information generated by the computer itself with the use of software. Interest calculations done automatically fall into this category. Hearsay evidence is records produced by the computer that are copies of information fed into the computer by humans initially. It is presumed that 'in the absence of evidence to the contrary the courts will presume that mechanical instruments were in order at the material time'. Section 65B of the Evidence Act 1872 has similar provisions introduced by the IT Act 2000. The other relevant authority in this respect is Uncitral Model Law, which states that electronic documents cannot be rendered inadmissible merely because it is electronic in nature. And the unreliability has to be independently proven. Further, even if certain documents are not real, they do become admissible, as documents are prepared in the ordinary course of business. The rationale for this presumption is that these entries are used for other purposes too and that is a sufficient guarantee of the truth of the records' content.

One would like to briefly touch on the certified copy aspects in the Bankers' Book of Evidence Act. If for some reason the evidence is not considered real then the question of a certificate may arise. We are of the view that if the programme is the one used in the course of business and if the software were functioning properly, then it may be sufficient to meet the requirements of admissibility.

The other difficulty comes because of the investigation techniques used. A physical act (say, a dacoit grabbing cash from a teller at gunpoint) would lead to an investigation as in any criminal act. The police would visit the scene of the crime, collect information from eye witnesses and try to gather finger prints or any trails left by the dacoit. In the case of a similar crime committed with the help of a computer the trail would be so far fetched that it might be necessary to get the cooperation of half a dozen systems managers and computer users. It could be an extremely difficult process. There are, of course, peculiar questions relating to privacy and the missing substitute for a biometric eyewitness testimony or physical evidence or the existing evidence pointing to a particular person. The only clinching evidence would be the recovery of the computer.

Perhaps, the time has come to harmonize the procedures in investigation and give a much greater leeway to the authorities in carrying out the investigations.

The Bankers' Book of Evidence Act, 1891, was amended in 2002 for acceptance of digital evidence. However, to get it accepted as evidence the following requirements have to be complied with. A printout of entry or a copy of a printout shall be accompanied by the following:

- A certificate to the effect that it is a printout of such entry.
- A certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of:
 - The safeguards adopted by the system to ensure that data is entered or an authorized person performs any other operation.
 - Safeguards adopted to prevent and detect unauthorized change of date.
 - Safeguards available to retrieve data that is lost due to systemic failure or any other reason.
 - The manner in which data is transferred from the system to removable media like floppies, discs or tapes or other electro-magnetic data storage devices.
 - Mode of verification in order to ensure that data has been accurately transferred to such removable media.
 - Mode of identification of data storage devices.
 - Arrangement and custody of such storage devices.

It would be extremely difficult to get such certificates and to bring the officers for cross-examinations.

To illustrate our point, e-details of a case in the UK has been discussed here. An American bank obtains unauthorized access to the confidential information contained in the website of a bank in the UK. The UK bank confirmed the details and telephoned the CEO of the US bank. The CEO laughed and is reported to have replied: 'We are doing you guys a favour by giving people access to your website.' When the bank asked its lawyers to review the case, some startling conclusions emerged: (a) since the UK bank was not complying with UK financial services and personal data protection laws, it might be the subject of compliance orders and fines; (b) alerting the national authority against an overseas hacker was not of much use; (c) the burden of proof in a criminal case in the US requires that a jury be persuaded beyond reasonable doubt that the defendant has committed an offence and securing the proof for such an act would be a formidable task; (d) the bank had to assess and gather evidence as to who owned the Intellectual Property Rights (IPRs) in the website. This would include the authors of its initial design because they would own it unless

the agreement with the bank stated that the bank was to be the owner. If they were acting as employees of the bank, the bank would own it. If however, they were acting as independent contractors, then each author would own whatever he or she had created.

A number of similar cases in the US can be referred to, where cyber crime and the subsequent treatment of these ‘criminals’ is not taken very seriously.

The waters get so muddy that institutions cannot be blamed for leaving the matters untouched. The solution would be for laws to be tailored to suit the requirements that are now emerging. It remains to be seen whether the laws will ever catch up with the rapid changes in technology. Commercial law is slow to catch up with the business malpractices.

Network Security

Security companies all over the world are locked in a race with malicious hackers to see who can react fastest to news of a new vulnerability. Increasingly, even the vandals are becoming more sophisticated. It is worth noting that net attacks are growing at the rate of 64 per cent per year. The year 2002 saw an enormous increase in such attacks. Every week, companies were attacked almost 32 times compared to 25 times per week in 2001. As if this was not enough, security companies hear about 400–500 new viruses every month and 250 vulnerabilities of computer programs. In fact, the losses suffered by these organizations are huge. The Computer Security Institute and the US Federal bureau of Investigation (FBI) computer crime and security survey shows that financial institutions are being continuously targeted and are not experiencing the scattergun approach. The survey also shows that more than 90 per cent of websites were attacked, 18 per cent suffered unauthorized access/abuse of their systems and 60 per cent had their sites vandalized. A further 80 per cent had suffered transaction thefts. The financial losses could well be in excess of US\$265 million. Of those surveyed, 16 per cent did not even know that they had a problem. Many employees who are familiar with the latest technologies can easily bypass the office systems, effectively, opening the back doors of the organization.

A list of most frequently attacked companies has the power, energy and financial institutions as its major constituents. There is, unfortunately, a tendency on the part of financial institutions to push such attacks or break-ins under the carpet and to prevent any adverse publicity. While the need for not causing an undue panic is appreciated, customers remain vaguely uneasy about such matters. At the cost of repetition, it is maintained that

customer anxiety on this point is a major stumbling block in the spread of e-banking. Banks and financial institutions must indicate exactly how they propose to tackle these problems and bring them to the notice of their clients. The time to plug holes is shrinking. In fact if they read the signs on the wall and move quickly, it would offer the Indian financial institutions a unique advantage.

The security concerns depend on the services offered. For the sake of analytical convenience these can be divided into three levels depending on the complexities of services offered. At level 1, the information provided could be tampered with and some data can be distorted. At level 2, the systems are interactive and they provide the ability to transmit sensitive messages, documents or files between users and financial institutions. At level 3, in addition to level 2 operations on the account, bill payments and other transaction services are included. These present a higher degree of risk. The use of an electronic channel to deliver products and services introduces unique risks due to the increased speed at which the systems operate and broad access in terms of geography, user groups and peripheral systems.

TYPES OF SECURITY FAILURES

The internet economy is built on information. In this economy, time is money and information is valuable. The value of e-finance is defined, in part, by technology's ability to move information and to affect markets quickly. The underlying assumption is that moving information is reliable. Reliability is based, in part, on constructing a system and a process that keeps the percentage of repudiated transactions to a minimum. In order to construct such a system, transactions must be appropriately authenticated, verified and authorized. A precursor to this is access controls. Access controls enable a dumb operating system to know whether an individual attempting to enter the system has been granted access. Authentication is the means used to assure the system that the party attempting to engage in an activity is, in fact, the party so designated. Verification is the means used to confirm that the party claiming a certain identity is the right party. Finally, authorization is the means used to determine that the party engaging in a transaction has the requisite authority to access that portion of the system or to engage in that type of activity. The value of information is based on its reliability and its integrity—whether the party was authorized to access or engage, whether the identity was authenticated, whether there is a risk of non-repudiation, whether there are any process restrictions for the particular transaction (specifically, whether the rules engine has any access

controls) and whether there are any relationship constraints (specifically, whether privacy or confidentiality is protected). The process restriction is an internal risk, and the relationship constraint is a potential legal liability. However, the value of any information is directly related to the extent to which the information meets these criteria versus the extent to which it needs to meet this criterion. So, on a scale of 1–10, if the information should be a 10 but the system can only ‘assure’ a rating of five, it has lost at least 50 per cent of its value. Thus, security is a value-added proposition and is a major business consideration.

Customer interaction with financial institutions is migrating from in person, paper transactions to remote access and transaction initiation. This migration increases the risks of doing business with unauthorized or incorrectly identified parties that could result in financial loss or reputation damage to the institution. Secure electronic service delivery is a key to providing consumers with improved, more flexible and convenient access to financial services and to enhancing the efficiency of banking operations. One of the challenges in implementing secure electronic service delivery is building the appropriate non-repudiation mechanisms into the banking platform. Reliable customer authentication is imperative for financial institutions engaging in any form of electronic banking or commerce. The risks of doing business with unauthorized or incorrectly identified individuals in an e-banking environment could result in financial loss and reputational damage through fraud, corruption of data, unenforceable agreements and the disclosure of confidential information.

In a world where people increasingly do business with virtual parties they have never met and will likely never meet, authentication becomes as integral to the transaction as the exchange of goods and tender. Yet, authentication is the Achilles’s heel of electronic finance. In fact, most computer intrusions are perpetuated as a result of insufficient access controls and weak authentication mechanisms. For example, in 1995, Citibank found itself in an ironic position: its technology was not as powerful as that of a group of hackers. Citibank’s main weakness was the use of ‘fixed passwords’ to guard its computerized cash management system. There is widespread concern, especially among those in the law enforcement community that the financial sector is not keeping up with the security side of technological change. For example, overall industry-wide use of passwords is outdated. In fact, a 1999 General Accounting Office (GAO) report highlighted the reality of outdated access controls; it found access controls to be at the forefront of security weaknesses. Beyond the norm of gates and guards that were often inadequate, failures of logical controls—those access controls built into software—were pervasive. In the information age, there are

hundreds of websites devoted to password cracking and/or interception. The most common programme used for password generation is Brute Force. This widely available application generates all alphanumeric combinations until the password is deciphered.

CONTROL DEVICES

There are two issues here: access and authentication. Access allows those who should be able to get onto the system for the purpose for which they are authorized. Authentication is assuring the system that the person trying to gain access or engage in a certain activity is, in fact, the person he or she claims to be and that the person is authorized to engage in the act. Used together and diligently, these processes are the most cost-effective security devices available. Financial institutions can use a variety of access and authentication tools and methodologies to authenticate customers. Existing access control techniques and authentication methodologies involve three basic factors:

- Something the user knows (for example, password or Personal Identification Number [PIN]).
- Something the user possesses (for example, ATM card, smart card or token).
- Something the user is (for example, biometric characteristic, such as fingerprint or retinal pattern).

An effective access and authentication programme should be implemented across the organizational structure, including affiliate entities, which requires the appropriate use of controls and authentication tools. Authentication processes should also maximize interoperability and offer consistency with the financial institution's assessment of the e-finance system risks. Before it goes online, the financial institution should examine its business processes, undergo a data classification inventory as part of its risk management analysis and configure its rules engines and access controls to support the data classifications.

ACCESS CONTROL USING PASSWORD AND PIN

The entry of a username or an ID and a secret string of characters such as a password or PIN is the most common and vulnerable of all single-factor authentication techniques. The effectiveness of password security depends

on three characteristics: length and composition, secrecy and system controls.

Even with these precautions, the inherent weaknesses of passwords are technology and time. As a result of increased processor speeds, patient hackers can acquire an encrypted password file or session. A program named L0ftCrack is a random character generation program that, when used with a 1.8 giga processor, can run 1 million keyboard combinations per second.

The computer will execute L0ftCrack in logical progression, thus making it a matter of time before that terminal is compromised. Note that hackers with criminal intent are patient. It may take months to set-up an attack, but it takes seconds to execute a successful intrusion on a bank. Passwords can be compromised and thus provide no real level of non-repudiation.

ACCESS CONTROL USING TOKENS AND SMART CARDS

A token is an authentication method that makes use of something the user possesses. Typically, a token is a two-factor authentication process, complemented by a password or a biometric as the other factor. The device itself may authenticate static passwords or biometric identifiers used to authenticate the user locally. This process avoids the transmission of shared secrets over an open network. Most so-called 'smart cards' are nothing more than a credit card sized device containing a microchip. The sophistication of the chips varies, but most commercially available implementations are far from being secure. In considering the threat posed by criminals, it is not enough to deter the casual criminal through the inconvenience of basic security. New measures must be able to withstand the continuous and repeated efforts of a determined and well-funded adversary. Standard smart cards usually contain account numbers, encryption keys and often additional stored information (such as biometric profiles), which can be extracted from the card and duplicated or altered. In doing so, the determined adversary can then present cloned or altered data smart cards as genuine, defeating the security and gaining access to critical infrastructure.

Cyoni™ technology is a core authentication system with a wide variety of applications. It is based on the use of mass-producible microchips that can be deployed in a variety of convenient consumer products. Each chip behaves uniquely in response to random or pseudo-random challenges. The system is fundamentally an authentication technology. The primary security advantage of Cyonic™ technology is that no system-level information is

contained on the microchip. Thus, even a determined adversary, upon destructive analysis of the chip, will gain no insight into the system-level functions that authenticate system users. This prevents any adversary from achieving successful account cloning, regardless of the adversary's technical or financial resources.

Biometric authentication techniques can grant or deny access to networks by automatically verifying the identity of people through their distinctive physical or behavioural traits. A biometric identifier represents a physical characteristic of the user. The identifier is created from sources such as the user's face or hand geometry, voice, iris (or retina) or fingerprint. Once 'captured', a biometric is translated algorithmically into a complex string of numbers and stored in a database as a template. Later, this template is compared to any 'live' biometric presented as proof of identity. Introducing a biometric method of authentication requires physical contact with each customer to initially capture and validate the biometric information. This corresponds to the 'know thy customer' mantra of the financial action task force principles.

Biometrics is the future of access controls. Biometric devices fulfill the non-repudiation element of layered security by authenticating a user by his or her physical characteristics. Implementing biometric technologies virtually guarantees a system administrator that the person who initiated the communication or system access was who he or she should have been. The greatest obstacle that biometric technology faces lies in the acceptance of the public. Many people fear the ramifications of storing personal information in a vast database. There is an apprehension (fuelled no doubt by books such as *1984* and *Gattaca*) that this might lead to unacceptable centralized control or interference, etc. We must say that not having such controls could lead to far greater risks. The e-financial world must evolve past our fears of 'big brother', in order to face the security challenges that will face all 'virtual' industries in the years to come. Authentication is the gargantuan cyber-loophole that is exploited more often than not in order to gain access to others' computer systems.

MALICIOUS ATTACKS

Worms, Trojans (the analogy is to the Trojan horse) and viruses are vehicles for deploying an attack. A virus is a program that can replicate itself by infecting other programmes on the same system with copies of itself. Trojans do not replicate or attach themselves to other files. Instead, they are malicious programs that are hidden within another program or file.

Once the Trojan file is executed, it can perform malicious activity at will. Virus scanners are critical in the mitigation of these attacks. Virus scanners should be updated every night. Beginning with an institution's email gateway, every inbound attachment should be scanned for viruses. File servers should be set to active scanning mode, where they scan every file copied onto them. Desktop scanners that protect the user's PC should also be updated. Data should be tested against standard loads if updates catch anything.

Worms, which are a relatively new phenomenon, use existing security vulnerabilities to gain access to the device. Worms replicate themselves onto other systems via a network connection. Typically, viruses and worms become malicious only when the infected files are accessed or deployed. Most of the time, these vulnerabilities can be eliminated by simply applying patches. The irony here is that someone who is not keeping up-to-date with patches most likely is not keeping up-to-date with virus software either. This human 'system' failure can have catastrophic implications for an institution's e-financial network.

DATA TRANSMISSION RELIABILITY

Cryptography and cryptographic tools sound complex and mysterious. The details of how these tools are constructed and work are intricate, laced both with mathematics and with provable and unprovable properties. The security of some tools can be based firmly upon some intractably difficult mathematical problem. The security of other tools cannot be proven formally, but is trusted as a result of the inability of experts to find and demonstrate any weaknesses in the tools over the years. However, what cryptographic tools do and how they are used are very easy to understand. There are only six basic types of cryptographic tools. They are:

- Symmetric (secret) key encryption.
- Asymmetric (public/private) key encryption.
- One way hash functions.
- Message authentication codes.
- Digital signatures.
- Random number generators.

By careful use of these cryptographic tools one seeks to design systems that can provide system security in the face of any of the attacks defined in an associated threat model.

ASYMMETRIC KEY ENCRYPTION

For asymmetric key encryption, the key used to encrypt data is a different key from that used to decrypt data. Unlike symmetric key encryption, which uses the same secret key both for encryption and decryption, asymmetric key encryption uses two different keys. Why is this important? It is important because only one of the keys needs to be kept private (or secret). The other key can be made public. It is for this reason that asymmetric key encryption popularly is called ‘public/private’ key encryption. Asymmetric ciphers greatly facilitate problems of key distribution.

One can appreciate the power of having two keys by considering how one orders items over the internet, such as books from Amazon.com. The ordering process used by such websites uses a protocol called Secure Socket Layer (SSL), to assure that a secure session is established between the customer’s computer and the website. An SSL session begins with a ‘handshake’ protocol. The customer’s computer sends a greeting to the Amazon web server, and web server’s reply includes a certificate containing an Amazon public key. The customer’s computer checks that the certificate is valid and then uses Amazon’s public key to encrypt data that both the user’s computer and the web server will use to construct a symmetric key for the session. Only the Amazon web server has the private key needed to construct the symmetric session key. After some further checking, the session continues using the symmetric key to encrypt/decrypt messages. The order information—credit card number, shipping address, gift-wrapping, greeting message and items ordered—then can be sent confidentially to Amazon.

The most widely used asymmetric cipher is called ‘RSA’, an acronym composed of the first letters of the last names of its inventors: Ron Rivest, Adi Shamir and Leonard Adleman, who first published their work in the summer of 1977. Patent protection for the algorithm expired in September 2000 and now it is in the public domain. RSA operates upon very large integers modulo, the product of two secret prime numbers. RSA public and private keys each are pairs of such large integers. For good security today, 1024 to 2048 bit integers are used, although some applications continue to use 512 bit integers. The cryptographic strength of RSA derives from the difficulty in finding the two secret primes given only their product.

Due to the relative strengths and weaknesses of symmetric and asymmetric cryptography, a common practice is to use asymmetric key cryptography for key distribution and symmetric key cryptography for the bulk of the transferred data. This is what is done within the SSL protocol— asymmetric

cryptography is used to establish a newly created symmetric key, which then is used for the data transfers within the SSL session.

USE OF RANDOM NUMBERS

Random numbers are employed throughout cryptographic algorithms and protocols. They are used for keys, challenge values, pre-hashing appendages for passwords, and so on. Hardware devices based on some form of physical randomness are also beginning to appear. The problem with such hardware devices, of course, is testing them to assure they are operating correctly.

Sole computational means for generating truly random numbers do not exist. A favourite quote of John Von Neumann's, cited by Bruce Schneier, is: 'Anyone who considers arithmetic methods of producing random digits is, of course, in a state of sin.' Fortunately, computational means do exist for computing numbers that are sufficiently unpredictable that they can be used in lieu of truly random numbers. Such numbers are called 'Pseudo-Random Numbers' (PRNs). Some of the pseudo-random number generation methods employ values obtained by physical measurements of random events in a computer system, such as typing rates, arbitrary mouse motions, arrival times of I/O (an authentication software) interrupts. Others are based on symmetric cryptography or the difficulty of hard mathematical problems such as the factoring problem. Pseudo random number generators (PRNGs) that produce sufficiently unpredictable values are called 'Cryptographically Strong Pseudo Random Number Generators' (CSPRNGs).

It is not easy for banks and financial institutions to safeguard their networks because new vulnerabilities are discovered daily, and their fixes/patches must be diligently applied to all systems. New connections to the internet, modems, and virtual private networks (VPNs) create a multitude of new access points to a network whose risk is defined by its weakest link. Penetration testing entails obtaining knowledge of existing vulnerabilities of a computer system or network, and using that knowledge to attempt to gain access to resources on the computer or network while bypassing normal authentication barriers. It may also include exploiting vulnerabilities to gain increased authorization—for instance, to go from regular user to super-user. Penetration testing is good only on the day it was done (this is true for all security testing). Penetration testing is an excellent way of testing installed security measures, policies and procedures, and the effectiveness of a company's end-user security training programmes. First, a company will be able to tell if security measures such as firewall and

Intrusion Detection System (IDS) are functioning properly and what skill level is required to circumvent them. Second, a company will gain insight into whether established policies and procedures allow its staff to detect and react to an intrusion properly. And third, a company can determine if additional training is required for its end-users. Penetration testing should be performed at least annually and more often if the system is subject to frequent application or operating system updates. Once a penetration test has been performed, ongoing vulnerability assessment should be performed to address newly discovered exploits. The frequency of the vulnerability assessment should be determined on the level of risk an organization is willing to accept. Given the speed at which new vulnerabilities and exploits are discovered, a vulnerability assessment should be performed semiannually and in many cases quarterly no matter what level of risk one is willing to accept.

So far the causes and steps the organizations can take as damage control have been outlined. The next section points out the most frequent lapses which occur and which are within the category of 'controllable' items from an organizational perspective.

MANAGERIAL CHECKLIST

Top 20 Red Flags

- Lack of training and expertise of administrators.
- No time for or interest in reviewing log files.
- No time for or interest in hardening machines.
- Deployment of new technology without security peer review.
- Failure to install software patches that fix security flaws.
- Lack of strict requirements to use strong passwords.
- Removal of security mechanisms because they cause user inconvenience. Restoration of systems from backups and failure to reload any patches that were previously installed.
- Failure to remove administrative-level accounts that were added temporarily for service personnel.
- Failure to install or use available security mechanisms such as password policy enforcement or system event logging.
- Lack of daily audit of network logs for suspicious activity.
- Setting up computer systems by using the default software. These default settings are designed to get the system booted up and run with the least interference; often these are very insecure.

- Failure to perform routine backups of systems and then test those backups for viability.
- Failure to properly install and update virus protection software.
- Sharing administrative accounts and passwords over multiple systems.
- Primary reliance on a firewall or public key infrastructure (PKI) system for security.
- Use of Simple Network Management Protocol (SNMP), telnet, file transfer protocol (ftp), mail, rpc, rservices or other unencrypted protocols for managing systems.
- Assignment of passwords to users over the phone.
- Failure to educate users about security problems and what to do when they see a potential problem.
- Poorly written and implemented policies and procedures.
- Improper documentation.

The following are some of the best practices prevalent in the industry.

Best Practices

- Network administrators should be responsible for installing and verifying patches and updates to operating systems weekly.
- On-site trained security staff should be present 24/7.
- Employees should be required to use robust passwords (long in length; mix of letters, numbers and symbols), which should be changed monthly.
- Computer monitors should not be visible to anyone who is not an employee of the institution.
- Network administrators should implement a profile procedure to process transfer of employees to another office in the bank, termination of employees and changing an employee's level of access within the bank's systems.
- Those who are responsible for large value transfers should utilize biometric identifiers as their password.
- Backups should be maintained of all critical material that is stored in a different location.
- An incident response capability and a plan that ensures continuity of operations and recovery from security breaches should be in place.
- Strong authentication—preferably biometrics, smart cards and cryptography—should be exercised for large value transfers.

- Firewalls and intrusion detection systems should be installed.
- Penetration testing/auditing should be performed on all of the institution's systems.
- A login banner should be displayed stating that the system is only for authorized use and is subject to monitoring.
- Patches must be updated weekly to both servers and remote access machines. See <http://www.microsoft.com/technet/security/current.asp>
- Critical operations should have two-person controls.
- A security policy should be developed that mandates training for non-IT staff vis-a-vis an incident response plan and that prohibits instant messaging, voice-over IP and wireless local area network (WLAN) installation without appropriate authorization and securitization.

INCIDENT RESPONSE

The ability to react quickly to security incidents is an essential part of an overall security plan. An organization's ability to operate will depend on its ability to provide timely information to its clients in the form of electronic data. It is also essential to categorize information. Information from critical systems will certainly receive a more direct and focused response than, for example, electronic information stored for office supplies. An organization needs the ability to react to and recover from security incidents as they arise with an effective and coordinated response, which in turn will minimize the cost and damage to the organization's infrastructure and image within the banking industry. A security incident can be defined as an event that changes the security posture of an organization or circumvents security policies developed to prevent financial loss and destruction, theft, or loss of proprietary information. It is characterized by unusual activity that causes the organization to investigate because the activity cannot be explained through normal operations. Some possible classifications for security incidents are:

- Virus attacks (unable to clean, rename or delete).
- Denial of service attacks.
- IDS alert notifications (false positives possible).
- Automated scanning tools.

Banking organizations must share in the responsibility of coordinating their response efforts with those of other financial institutions. Networking in a trusted environment and sharing incident information and detection/response techniques can be important to all of these organizations in identifying and correcting weaknesses. Gathering intelligence information from all sources is a critical part of information infrastructure protection. Having an information-sharing network in place can also help government agencies alert other agencies to potential and/or actual threats directed at the critical information infrastructure of nations.

Incident response within any organization must begin with management. Management is responsible for providing the support, tools, personnel and financial backing needed to ensure the success of the incident response team. An incident response team must be perceived well by all concerned. Security awareness training and briefings for senior management are key components of a successful deployment of an incident response team.

Monitoring systems and reviewing security alert information submitted by vendors is an important part of an incident response team's proactive duty. IDS systems, however, do not provide a complete solution to identifying and responding to incidents. An overall security plan is needed to ensure overall protection that would include an incident response mechanism. An incident response team must also develop procedures. Clear definitions of each type of incident will enable members to react quickly and effectively. Procedures must detail the steps team members should take when alerted about an incident. Included within the procedures must be clearly defined investigative goals to be achieved before an incident can be closed. The team should also list and post contact information of key personnel and management to notify.

SURVIVABLE SYSTEM DEVELOPMENT

Survivability analysis or business continuity helps to identify the essential functions or assets in the institution that must survive in the event of an attack or system failure. The delivery of essential services and the preservation of essential assets during a compromise, and the timely recovery of full services and assets following attack are among these functions. The organizational integration phenomenon that typifies the modern banking community is accompanied by elevated risks of intrusion and compromise.

It is essential to determine what elements in the institution's IT infrastructure are absolutely mission-critical—that is, what elements must be up

and running within a certain time in order for business to continue. One must envisage various compromises to the system so that contingency plans are there to cover all potential threats. The following sources on survivability will assist network architects in determining the impact of certain accepted risks.

The Carnegie Mellon Software Engineering Institute Network Systems Survivability Program uses incident data collected by the CERT (http://www.cert.org/nav/index_purple.html) as a basis for the institute's survivability research and for trend identification and the prediction of future problems.

The European Dependability Initiative (<http://www.cordis.lu/esprit/src/stdepnd.htm>) represents a major research effort within the European Union to address the critical infrastructure protection and survivability efforts of the member nations. There are plans for joint US/EU cooperation.

The National Infrastructure Protection Center (NIPC) is the US government's focal point for threat assessment, warning, investigations and response to attacks (<http://www.nipc.gov>).

E-SECURITY IN THE CASE OF WIRELESS NETWORKS

Wireless networks are available in three basic formats: high-powered microwave systems used by telephone companies for long-haul, line-of-sight communications; Code Division Multiple Access/Time Division Multiple Access/Global System for Mobile Communication (CDMA/TDMA/GSM) cellular and PCs networks used for wireless phones and personal digital assistants (PDAs); and wireless LANs that uses the 802.11b protocol. While all of these are common throughout the world, they all suffer from the same basic security flaw. They use radio frequency (RF) technology to transmit their information. The result can be compromising of their transmissions. Wireless networks (WLANs) have seen explosive growth in their deployment. With cost savings at an all-time high and with the simplicity of installation, WLANs have been deployed rapidly. Wireless networks were supposed to do what traditional Ethernet LANs do without cables. Convenience for the customer is paramount in the proliferation of wireless. Wireless technology is built around the 802.11b IEEE standard in the US and the GSM standard in Europe. The next section discusses the security issues raised by both of these forms of cellular technology and provides a glimpse into the future of third generation wireless (3G).

MANAGER'S LAPTOP—THE BIG PROBLEM

Wireless LANs make use of the IEEE 802.11b technology, which is a system that transmits and receives in the 2.4GHz range and is capable of a maximum network capacity of 11Mbps. WLANs implement the Wireless Equivalent Protocol (WEP), which was designed to offer the same security features as a physical wire: confidentiality, access control and data integrity. 2001's Black Hat Briefing made public that hackers have a multitude of ways in which they can crack, intercept or modify WEP messages on a wireless network. There is a particular problem with devices using the 802.11 wireless network standard. The encryption can easily be broken, and once broken it can provide easy access to corporate networks for anyone listening in. Furthermore, if a wireless gateway is located on the corporate Ethernet network, that network will broadcast all the data passing through it over the airwaves. If someone cracks the encryption, that person can intercept everything. But the immediate points of vulnerability are the mobile devices themselves, including notebooks, which tend to be poorly protected and which often contain sensitive, but unencrypted data. The danger to financial and corporate networks is very real.

When designing a wireless network, one should keep in mind a number of important security concerns. These are the six basic categories of wireless network security risks:

- **Insertion attacks**—The intruder attempts to insert traffic into your network, typically through an unsecured mobile access point.
- **Jamming**—This is a DoS (denial of service) attack, where the attacker tries to flood the radio frequency spectrum of your wireless network by broadcasting packets at the same frequency as your network.
- **Encryption attacks**—The IEEE 802.11b wireless network standard uses a WEP encryption method. This standard uses weak encryption and initialization vectors and has been cracked successfully many times.
- **Traffic interception and monitoring** (war driving)—Wireless packets using the 802.11b standard have an approximate transmission distance of 300 feet. This means that anyone with the proper standard equipment can receive that signal if he or she is in transmission range. Equipment to extend that range further is easily available, so the area of interception can be quite large and hard to secure properly.

- **Mobile node to mobile node**—Most mobile nodes (laptops, PDAs) are able to communicate directly with each other if file-sharing or other TCP/IP services are running. This means that any mobile node can transfer a malicious file or program rapidly throughout your network.
- **Configuration issues**—Any wireless device, service or application that is not correctly configured before installation and use can leave an entire network at risk. Most wireless devices and applications are preconfigured to accept any request for services or access. This means any passing mobile client can request and receive telnet sessions or ftp.

WAR DRIVING

Industrial espionage and white-collar crime have reached new heights with the advance of new technologies. War dialing, the hacking practice of phoning up every extension of a corporate phone network until the number associated with the firm's modem bank is hit upon, has been replaced by war driving. War driving involves motoring between targeted financial institutions and corporate headquarters with a laptop fitted with a WLAN card and trying to record network traffic (sniffing). According to Dave Thomas, the Chief Investigator of the FBI Computer Crimes Division, war driving is a widespread phenomenon that jeopardizes the security of all institutions and corporations that implement WLANs.

When testing and deploying WLANs, a network administrator may find that the institution's laptops can only connect to the access points within a certain distance and may, therefore, assume that the signals do not travel beyond this point. This is a flawed assumption. In fact, these signals may travel for several thousand metres if there is nothing in the way to deflect or interrupt the signal. The reason for this misconception is that the small antennas in the laptops cannot detect the weaker signals. But if external antennas are used, the range can be vastly extended. The wireless segment is usually omnidirectional, so a potential adversary need not gain physical access to the segment to sniff (or record) the packet traffic. As a result, WLANs are susceptible to message interception, alteration and jamming. These considerations raise the issue of how to secure wireless networks better. This will be as critical as securing fixed-line internet systems in the emerging markets, as highlighted previously.

Each of these security breaches and associated risks can be minimized or negated with the proper use of security policy and practices, network

design and system security applications, and with the correct configuration of security controls.

THE EUROPEAN CELLULAR STANDARD: GSM

In 1982, the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Groupe Spécial Mobile (GSM) to study and develop a pan-European public land mobile system. Today, GSM is the world's most widely deployed and fastest growing digital cellular standard. GSM subscribers worldwide number nearly 600 million, more than two-thirds of the world's digital mobile population. The numbers are increasing by four new users per second. GSM covers every continent, being the technology of choice for 400 operators in more than 170 countries. However, this is only the beginning of the wireless revolution. The industry predicts more than 1.4 billion GSM customers by the end of 2005. GSM phones have a small smart card inside them that holds the identity of the cell phone. This small smart card is called a Subscriber Identification Module (SIM). The SIM keeps the identity secret and uses cryptography to protect it.

GSM VULNERABILITIES

SIM Card Vulnerability

In both European and American GSM systems, the network access method is the same. Removable smart cards in the phone (SIM cards) are used to store phone numbers, account information and additional software such as wireless web browsers. The data on the cards is encrypted, but the COMP128 algorithm that protects the information on the card has been compromised, making these cards susceptible to duplication. War driving is not a substantial issue for cellular subscribers using GSM. Regardless of frequency, cellular signals can easily be jammed. There is a widely known method for recovering the key for an encrypted GSM conversation in less than a second using a PC with 128 MB of RAM and 73 GB of hard drive space. The security of GSM phone technology is limited. It is possible to clone GSM SIM cards. The hack attack is possible because critical algorithms are flawed, making it possible to dump the contents of the SIM cards and then emulate them using a PC.

This latest problem could render GSM phone conversations totally insecure. For a bank, there are other issues. For example, a remote teller

machine could be tricked into communicating with a fake mobile tower because it cannot reach a real one. This would allow the perpetrator to remotely control the transmissions of funds via the teller machine. Thus, a modified GSM cell phone and laptop can be made to act as a base station. All that is necessary is to make a few software and hardware modifications to the phone and to be within closer range than the actual tower. The mobile phone must authenticate itself to the base station, but the station does not have to authenticate to the phone at all.

The SMS Vulnerability

Short Message Services (SMS) is used in GSM systems for many reasons, such as voicemail notification, updating the subscriber's SIM, sending short text messages and communicating with email gateways. Although these services are convenient, they pose an additional risk to the security of the network. There is freely available software that can spoof SMS messages, send SMS bombs to both handsets and SMS gateways (used to communicate between devices both on and off the network) and corrupt SMS packets that can crash the software on most handsets.

The GPRS Vulnerability

General Packet Radio Service (GPRS) is an IP packet-based service that allows an always-on connection to the internet. The main problem with this is that it still relies on SMS for Wireless Application Protocol (WAP) push requests. A spoofed (cloned) SMS packet can be sent to the phone requesting a redirected site and fooling users into entering their information into a fake site that they believe is a secure order form. Many GPRS-enabled phones also support Bluetooth, IBM's wireless programming language.

Each Bluetooth device has a unique address that allows users to have some trust in the person at the other end of the transmission. Once this ID is associated with a person, by tracking the unscrambled address sent with each message it is possible to trace individuals and easily log their activities. For Bluetooth devices to communicate, an initialization process uses a PIN for authentication. While some devices will allow you to punch in an ID number, you can also store a PIN in the device's memory or on a hard disk. This is highly problematic if the physical security of the device cannot be guaranteed. Also, most PINs use four digits and half the time they are '0000'.

WAP Weaknesses

The common flaw in any of these devices, no matter what network, is the Wireless Application Protocol standard, which also includes Wireless Markup Language (WML) and Handheld Device Markup Language (HDML). For the sake of convenience, developers try to require the least amount of keystrokes when entering credit card number or personal or account information. This means that most of this information is still stored on a server, but the password to access that server is stored in a cookie on the handheld device, requiring only a PIN or sometimes nothing at all to shop online or transfer funds. This means that the actual mechanism used to transport sensitive information end-to-end in these untrusted public cellular networks, is left to Wireless Transport Layer Security (WTLS). Unless 128-bit SSL for mobile commerce or IPSEC for Enterprise access is being used, which most handsets cannot support because they lack processing power and bandwidth, there will be a weak link somewhere in the network that can be exploited. Even then, this only pushes the weakness out to the end devices that are communicating and it can be easily lost. GSM uses the Wired Application Protocol and also the Wireless Transport Layer Security. This is equal to Secure Socket Layer, but it has weaker encryption algorithms. WTLS is not compatible with SSL, which is the industry standard. Wireless messages travel through a 'gateway' that channels them to a wired network for retransmission to their ultimate destination. At the gateway, the WTLS message is converted to SSL. For a few seconds, the message is unencrypted inside the gateway, which in turn makes the communication vulnerable to interception.

Security Solutions for GSM

The inherent problems affecting GSM are not easily corrected. The telephones and PDAs that use GSM technology typically cannot upload protective firmware and software. Users are at the mercy of the telephone developer. Whereas GSM is not vulnerable to war driving like its American counterpart, 802.11, it is suffering from several core vulnerabilities. The 802.11 standard is geared to computers, not handhelds and, thus, security can be improved much more drastically for 802.11 than for the GSM protocol. Virtual private networks are the common thread between the two. The establishment of VPNs is commonly referred to as the solution for the existing vulnerabilities of GSM and 802.11. However, when it comes to proper layered security, there are no magic bullets.

To protect information systems that may use any of these technologies, users should deploy virtual private network technology at each and every trusted gateway into their networks and ensure that every user accessing the trusted network uses Virtual Private Network (VPN) technology. A VPN is essentially a private connection between two machines that sends private data traffic over a shared or public network, the internet. VPN technology lets an organization securely extend its network services over the internet to remote users, branch offices and partner companies. In other words, VPNs turn the internet into a simulated private wide area network (WAN). VPNs allow remote workers to access their companies' servers.

SOUND PRACTICES FOR MANAGING OUTSOURCED E-BANKING SYSTEMS AND SERVICES

- E-finance organizations should adopt appropriate processes for evaluating decisions to outsource e-finance systems or services.
- Bank management should clearly identify the strategic purposes, benefits and costs associated with entering into outsourcing arrangements for e-banking with third parties.
- The decision to outsource a key e-finance function or service should be consistent with the organization's business strategies, should be based on a clearly defined business need and should recognize the specific risks that outsourcing entails.
- All affected areas of the bank need to understand how the service provider(s) will support the organization's e-finance strategy and fit into its operating structure.
- E-finance companies should conduct appropriate risk analysis and due diligence prior to selecting an e-finance service provider and should continue with it at appropriate intervals thereafter.
- Organizations should consider developing processes for soliciting proposals from several e-finance service providers and should also develop a criteria for choosing among the various proposals.
- Once a potential service provider has been identified, the bank should conduct an appropriate due diligence review, including a risk analysis of the service provider's financial strength, reputation, risk management policies and controls, and ability to fulfill its obligations.

- Thereafter, banks should regularly monitor and, as appropriate, conduct due diligence reviews of the ability of the service provider to fulfill its service and associated risk management obligations throughout the duration of the contract.
 - Banks need to ensure that adequate resources are committed to overseeing outsourcing arrangements supporting e-banking.
 - Responsibilities for overseeing e-finance outsourcing arrangements should be clearly assigned.
 - An appropriate exit strategy for the organization to manage risks should a need to terminate the outsourcing relationship arise.
- Organizations should adopt appropriate procedures for ensuring the adequacy of contracts governing e-finance. Contracts governing outsourced e-finance activities should address, for example, the following:
 - The contractual liabilities of the respective parties as well as responsibilities for making decisions, including any subcontracting of material services are clearly defined.
 - Responsibilities for providing information to and receiving information from the service provider are clearly defined. Information from the service provider should be timely and comprehensive enough to allow the organization to adequately assess service levels and risks. Materiality thresholds and procedures to be used to notify the bank of service disruptions, security breaches and other events that pose a material risk to the bank should be spelt out.
 - Provisions that specifically address insurance coverage, the ownership of the data stored on the service provider's servers or databases and the right of the organization to recover its data upon expiration or termination of the contract, should be clearly defined.
 - Performance expectations, under both normal and contingency circumstances, are defined.
 - Adequate means and guarantees, for instance through audit clauses, are defined to insure that the service provider complies with the bank's policies.
 - Provisions are in place for timely and orderly intervention and rectification in the event of substandard performance by the service provider.

- For cross-border outsourcing arrangements, determining which country laws and regulations, including those relating to privacy and other customer protections, are applicable.
- The right of the organization to conduct independent reviews and/or audits of security, internal controls and business continuity and contingency plans, is explicitly defined.
- Organizations should ensure that periodic independent internal and/or external audits are conducted of outsourced operations to at least the same scope required if such operations were conducted in-house.
- For outsourced relationships involving critical or technologically complex e-banking services/applications, organizations may need to arrange for other periodic reviews to be performed by independent third parties with sufficient technical expertise.
- Organizations should develop appropriate contingency plans for outsourced e-finance activities.
- E-finance companies need to develop and periodically test their contingency plans for all critical e-banking systems and services that have been outsourced to third parties.
- Contingency plans should address credible worst-case scenarios for providing continuity of e-banking services in the event of a disruption affecting outsourced operations.
- Companies should have an identified team that is responsible for managing recovery and assessing the financial impact of a disruption in outsourced e-banking services.
- Companies that provide e-finance services to third parties should ensure that their operations, responsibilities and liabilities are sufficiently clear so that serviced institutions can adequately carry out their own effective due diligence reviews and ongoing oversight of the relationship.
- E-finance companies have a responsibility to provide serviced institutions with information necessary to identify, control and monitor any risks associated with the e-banking service arrangement.

There are many issues and alternatives associated with the best implementation method. It is hoped that over a period, a dominant industry-wide standard would appear. At the same time, even the most straight

forward solutions available need to be monitored and maintained and patched on a regular basis to be effective. Ultimately organizations need to look at their own risk management issues and decide what level of vulnerability they can afford. It must be kept in mind that damage levels are rising to a point where security concern cannot be taken lightly. Further, banks must come out openly and make their clients aware about the occurrence of incidents. Information leaks through some sources within the organization would make matters worse. It would be better to come clean and advise the clients about the steps proposed. Agreements and the fine print therein may make it difficult for the clients to force the banks to make good the losses, but these are not helpful in building confidence levels. Ultimately the clients' trust is what matters in a highly leveraged industry.

Cyber Laws

The fundamentals of e-commerce and finance rests mainly on the legality of e-contracts entered into between two or more parties. The rules and regulations are embodied in the Indian Contract Act, the Evidence Act, the Civil Procedure Code, the RBI Act 1934, the Bankers' Book of Evidence Act, and so on. However, all these embody rules regarding manual operations and paper-based documents.

Generally, commercial practice moves a few paces ahead of the statutes and it takes time for the laws to catch up. The same is true in a large measure about e-finance and e-commerce. The whole gamut of activities is yet to take deep root in the socio-commercial policy and with rapid technological advances being the order of the day; the lags are bound to be prevalent.

The earlier edition of this work concentrated more on legal provisions and the difficulties in bringing about parity between paper documents, manual procedures and their acceptability as evidence. During seminars and discussions, many participants wanted to know details regarding specific aspects like digital signatures, web penetrations, security lapses and enforcement of documents. Further, the changes introduced to Bankers' Book of Evidence Act, Contracts Act, and so on, were areas of concern rather than the broader aspects of the IT Act of 2000. Accordingly, this chapter has been tailored to suit these requirements and also to bring out the relevant features of the IT Act that are of great concern to the practicing financial services.

The incidence of cyber law pervades a number of areas, but we would concentrate on the following five aspects:

- The Contract aspect.
- The Intellectual Property aspect.
- The Security aspect.
- The Evidence aspect.
- The Criminal aspect.

In a sense 'cyber law' encompasses the whole gamut of legal statutory provisions that affect computers and computer networks. It concerns individuals, corporate bodies and institutions which

- are instrumental for entry into cyber space;
- provide access to cyber space;
- create the hardware and software which enable people to access cyber space and
- use their own computers to go online.

Potential litigants include telephone provider companies, regulatory agencies, personal computer companies, software companies, academic bodies and firms that have a presence on the internet.

Before proceeding further, it is necessary to mention that the technology scene is changing too rapidly for any legal provisions to keep pace with the changes. One hopes that the courts would give the legislation a much broader base than could be envisaged by the framers. We begin by looking at some of the future developments, which would have to be reckoned within the near future. The one thing that strikes even a casual observer is the new capabilities in processing speed, transport and storage. The constraining influence of bandwidth is beginning to diminish. Data can be moved far more efficiently than before. We may perhaps reach a stage where anything that can be digitized is delivered to any number of users and that too at negligible costs. The marginal cost of transport is zero.

Network technology is being used for an ever-growing number of tasks as we shift away from today's PC-based model. The desktop computer is becoming only one of the many platforms for accessing networks such as the internet. There would be small, lighter devices optimized for basic activities such as email, text communication, and so on. The 'language' used helps in turning these machines smarter. Computers and communication equipment communicate with each other and move in and out of the many networks of the infrastructure. Softwares can and do take over the tasks, which, normally, humans would have to perform. They connect to local networks, manage the flow of information and negotiate with other applications to achieve the tasks.

The impact of such changes on the economics of the internet has been considered in the chapter on internet economics. The following paragraphs would detail the specific aspects of law touched on earlier.

QUESTIONS OF JURISDICTION

The first question that causes tremendous problems to the litigants is to have some understanding of a very perplexing issue of the scope of a court's power to hear particular disputes and to compel the parties involved to obey its commands.

It would be useful to mention that questions of jurisdiction are territorially based and they are difficult to translate to the internet. The word jurisdiction means many things and the broad umbrella of concepts that are covered can be summarized as follows:

- Power to legislate.
- Ability to serve the defendants a notice.
- Power to hear.
- Power to adjudicate.
- Subject matter of adjudication.
- Choice of law.
- Enforcement of judgments.

A brief discussion of Delhi High Court's judgement in the 'Banyan Tree' case is given below. The interested readers can find an exhaustive analysis of the case on the internet (spicyipindia.blogspot.com/2008/09/delhi-highcourt-considers-questions-of.html). Our purpose in citing the Indian case law is to demonstrate to the readers the complexity of issues, which otherwise appear to be simple. Further, it would be necessary to refer to case laws from countries like Canada, Australia, UK or the US. The issues are being examined from various angles and newer aspects are being considered. These cannot be ignored and would, over a period, fit some of our cases better than the body of decisions developed so far. All such matters have a vital bearing on the developments and students should pay attention to these aspects also.

Rather than going into a detailed review of case law it would suffice to mention some pertinent issues that have come up. Jurisdiction on the internet is an all-pervasive issue. Regardless of what substantive legal issue one is dealing with, whether it is intellectual property or privacy, jurisdiction issues would be key elements of that litigation. It would not be wrong to say that the internet is one big jurisdictional problem.

Events on the Internet occur everywhere but nowhere in particular. Communications are engaged in by online personae who are human and real, but who are unreal in that they might not be traceable to any particular person. No physical jurisdiction has a more compelling claim than any other to subject these communications and events exclusively to these laws. (Post and Johnson 1996)

THE CONTRACT ASPECT

The central point to remember is that the internet is a medium or a collection of media, which can be used for contracting. The law developed so far, does cover all the new elements it has been confronted with, but the law as it applies to the internet is far from settled yet.

Perhaps, the most suitable approach on the subject is Lord Denning's judgement in *Entores Limited vs Miles Far East Corporation*. The relevant portions of the judgment have been quoted for the readers to develop the right perspective.

When a contract is made by post it is a clear law throughout the common law countries that the acceptance is complete as soon as the letter is put into the post box, and that is the place where the contract is made. There is no clear rule about contracts made by telephone or by telex. Communications made by these means are instantaneous and stand on a different footing The contract is complete only when there is acceptance of the offer. Any failure in hearing would result in the contract not being accepted. Same is the case when messages sent through teleprinters or telexes do not reach due to some failure of the system. The contract gets completed only when the messages are repeated and a proper acceptance received ... In all the instances, the man who sends the acceptance knows that it has not been received or that he has reason to know it. But suppose he thinks that it has been received. — The offerer in such cases is bound because he will be stopped from saying that he did not receive the message. (Lord Denning, *Entores Limited vs. Miles Far East Corporation*, 1955)

So far it has been assumed that the parties are present. The more likely events are that communication would be between the principals through the machines or through fax/email. However, it is possible that the senders and recipients may not be the principals, but servants with limited authority. The messages may have been sent out of office hours or there could be some default or defects at the recipient's end.

These difficulties can be constantly multiplied, but it has to be assumed that in the normal course of business, an acceptance sent by email/telex

should be treated as if it were an instantaneous communication between principals like a telephone conversation. Once the message has been received it is to be assumed that it has been delivered. The acceptor should take the required precautions to see that the acceptance is duly received. In conclusion, it could be said that: The 'offer' and 'acceptance of an offer' may be expressed by means of electronic records. As between the 'originator' and the 'addressee' of an electronic record, the expression/declaration of an intention or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record. The concept of an 'Originator and Addressee', 'Acknowledgement of Receipt' and concepts of 'Time and Place of Despatch and Receipt' are dealt with in a genuinely different way and need to be highlighted.

1. Unless otherwise agreed to between the originator and the addressee the despatch of an electronic record occurs when it enters an information system outside the control of an originator.
2. Save or otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows:

If the addressee has designated a computer source for the purpose of receiving electronic records: (a) receipt occurs when the electronic record enters the designated computer resource and (b) if the record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee.

The preceding section is not a complete reproduction of section 13 of the Information Technology Act. It has been included merely to stress the difficulties encountered in bringing about a functional equality.

THE 'FUNCTIONAL EQUIVALENT' APPROACH

The Model Law is based on a recognition that legal requirements prescribing the use of paper-based documentation constitute the main obstacle to the development of modern means of communication. The attempt was to overcome the impediments to electronic commerce by way of an extension of the scope of such notions as 'writing', 'signature' and 'original' with a view to encompassing computer-based techniques. Such an approach was used in a number of existing legal instruments, for example, in Article 7 of Model Law on Commercial Arbitration or in United Nations Commission

for Contracts for International Sale of Goods. It was also necessary to provide for developments in technology and communications applicable to trade laws without necessitating the wholesale removal of paper-based requirements or disturbing the underlying concepts.

The Model Law relies on an approach referred to as the 'functional equivalent' approach, which is based on an analysis of the purposes and functions of the traditional paper with a view to determining how these purposes or functions could be fulfilled through electronic techniques. Paper documents can be read, copied, preserved and would remain unaltered over time.

An electronic recorder can perform all these functions with a greater degree of reliability. The Model Law does not attempt to define a 'computer based' equivalent to a paper document. Instead, it singles out basic functions of paper-based form requirements with a view to providing criteria, which once met, enable the data-based messages to enjoy the same level of legal recognition as paper documents performing the same functions. The purpose in outlining the equivalence was to bring forth what the act was attempting, rather than be exhaustive.

The Information Technology Act 2000 is similar to the Model Law and the preamble acknowledges this fact.

An act to provide legal recognition for transactions carried out by means of electronic communication, commonly referred to as electronic commerce which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government Agencies and further to amend the Indian Penal Code, 1860, the Indian Evidence Act 1872, the Bankers' Book of Evidence Act 1891 and the RBI Act of 1934. (IT Act 2000)

The Act was passed to give effect to the resolutions of the United Nations General Assembly and to promote efficient delivery of government services by means of reliable electronic records.

We would now deal with one particular aspect viz. digital signatures and information security. The previous chapter dealt with security aspects at some length. This section will be restricted to problems of digital signature as a case of encrypted authentication. How a digital signature is created and how it achieves the same functionality as a hand written signature requires detailed explanation.

The Asian School of Cyber Laws defines digital signatures as 'an application of asymmetric cryptography'. Cryptography is the art of using codes and algorithms to scramble text so that it appears random to statistical

tests and can, therefore, be read by specified individuals only. It would be obvious that any communication in e-commerce transactions needs to be confidential, must not be altered in transit and must have adequate authorization. Further, the contract agreement should necessarily have restricted access, certification about the genuineness of such a document and the time when it was sent. Also, any unauthorized entity viewing such a document should not become aware of the parties to these transactions. Apart from these there must be no repudiation of the document sent. Nor should it be possible to revoke it.

Any cryptographic method in transferring documents necessitates the use of keys to decode the message. Digital signatures rely on 'Asymmetric Cryptography'. The system involves use of a pair of keys: a public key which encrypts data and a corresponding private key for decryption.

The creation of digital signatures could be explained as a series of steps.

- A message is written.
- The message is encoded, the hash function takes a message of variable length and produces an output of a fixed length. If the information is changed even by one bit an entirely different value output is produced.
- The message is sent.
- The message is received and a key relating to the original algorithm is used to decode it.
- The message is then read.

Steps 2 and 4 are carried out with the help of a software sent by the sender.

On receipt of the message, the receiver computes the digest of the original message with the help of a hash function used by the sender. He then uses the sender's public key on the digital signature to compute another message digest. The receiver then compares the original with the message already obtained and only when it is identical is it proved that they are digitally signed by the sender and that the message is not altered. The need for all this arises because it is necessary to ensure that the message is not altered.

However, one has to be wary of what could be described as man-in-the-middle attack. You have to be sure that the public key is genuine and not a forgery. One way of solving the problem is to get a certificate which comes with a public key that helps one to verify that the key is genuine. Countries

like Germany and Sweden have elaborate procedures and precautionary requirements in place that are met by the certifying authorities. The legal issues, which would otherwise have complicated the whole question, have to some extent been resolved by the procedural guidelines.

Following are the detailed provisions regarding the status of certification under Indian law:

Certification authorities will be controlled by a controller who will be appointed by the central government. The duty of the controller would be to license, certify, monitor and oversee the activities of the certification authorities. Certificates issued by foreign authorities would be recognized in India if the laws of such a country have a level of reliability at least equivalent to that required in India.

It is likely that over a period of time, a number of vendors may come into the picture. Owing to the initial and on-going costs, it is unlikely that banks will opt to develop their own digital signatures and would have perforce to depend on outsourcing or purchasing this capability for their existing infrastructure.

A number of vendors are likely to emerge. Unfortunately, such vendors might market proprietary solutions that may not be compatible with the bank's other systems. Inter-operability now and in the future should be a primary consideration. Gartner Group estimates that 30–40 per cent of public key infrastructure deployments will fail within two years of launching because they fail to demonstrate value.

The trust placed in banks may lead to their setting up in the near future, a Certification Authority (CA) organization or could well find themselves using digital signatures that are unverifiable or information systems that have no technical support. Banks and financial institutions must perform a thorough check of the vendor who intends to provide a digital signature solution.

It needs to be emphasized that implementing the use of digital signatures requires adopting a new or augmented set of technologies, services and bank policies. Implementing digital signatures means implementing digital documents and associated requirements for document management, storage, access security, periodic hardware upgrades and disaster recovery facilities. Implementing digital signatures also leads to maintaining digital records and service digital documents.

Use of digital documents implies reasonable access being provided to the customers. Further, if remote access is to be provided, a secure information area will have to be provided.

A whole set of new issues come up when a bank decides to become a CA. The primary role of a CA is to issue and verify digital certificates.

There are some complex liability issues. Additionally hardware and software will become obsolete. The bank must upgrade and replace older equipment. The nature of 'second' documents would raise question about their admissibility. In any proceedings involving a secure electronic record, it shall be presumed, unless evidence to the contrary is adduced, that the secured document is not altered since the specific point of time from which the record gained secure status.

The fact whether a secure procedure is commercially reasonable or not, shall be determined having regard to the procedure and the commercial circumstances at the time the procedure is used.

EVIDENCE ASPECT

This section will look into the question of acceptability in civil law cases. The detailed provisions have been deliberately quoted as bank and financial institution staff are very often required to present such documents in courts and it is necessary to have a proper understanding of the relevant provisions.

According to Articles 6, 7 and 8 of UNCITRAL Model Law, information shall not be denied legal effects, validity or enforceability solely on the grounds that it is in the form of a data message. Where the law requires information in writing, the requirement should be met by a data message if the information contained therein is accessible so as to be usable at a later date.

Article 9 of the Model Law provides the following regarding admissibility of evidence.

In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of an electronic data message OR (b) if it is the best evidence that the person adducing it could be expected to obtain on the grounds that it is not in its original form i.e., information in the form of a data message shall be given due evidential weight.

Of course, reliability of the manner in which the message was generated, stored or communicated, and the reliability of the manner in which its originator was identified, are the kind of factors that would be taken into account. The specific provisions contained in the IT Act 2000 relating to these aspects have been discussed in the following pages:

THE INDIAN IT ACT, 2000

Schedule II Information Technology Act, 2000—31*

Schedule II

(Section 91)

Amendments to the Indian Evidence Act, 1872

1. In Section 3,
 - (a) in the definition of 'Evidence', for the words 'all documents produced for the inspection of the Court', the words 'all documents including electronic records produced for the inspection of the Court' shall be substituted;
 - (b) after the definition of 'India', the following shall be inserted, namely, 'the expressions "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 1999'.
2. In Section 17, for the words 'oral or documentary', the words 'oral or documentary or contained in electronic form' shall be substituted.
3. After Section 22, the following section shall be inserted, namely:
'22A. When oral admission as to contents of electronic records are relevant.'
Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.'
4. In Section 34, for the words 'entries in the books of account', the words 'Entries in the books of account, including those maintained in an electronic form' shall be substituted.
5. In Section 35, for the word 'record', in both the places where it occurs, the words 'record or an electronic record' shall be substituted.
6. For Section 39, the following section shall be substituted, namely:

* The amendments to IT Act 2008 could not be included in this book since the President's assent was not received when this book was sent for printing.

‘39. What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers.

When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made.’

7. After Section 47, the following section shall be inserted, namely:

‘47A. Opinions as to digital signature when relevant.

When the court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact.’

8. In Section 59, for the words ‘contents of documents’ the words ‘contents of documents or electronic records’ shall be substituted.

9. After Section 65, the following sections shall be inserted, namely:

‘65A. Special provisions as to evidence relating to electronic record.

The contents of electronic records may be proved in accordance with the provisions of Section 65B.’

65B. Admissibility of electronic records.

- (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.
- (2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:

- (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;
 - (b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;
 - (c) throughout the material part of the said period, the computer was operating properly or, if not, then in any respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents and
 - (d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.
- (3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computer, whether—
 - (a) by a combination of computers operating over that period;
 - (b) by different computers operating in succession over that period;
 - (c) by different combinations of computers operating in succession over that period or
 - (d) in any other manner involving the successive operation over that period, in whatsoever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.
- (4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,

- (a) identifying the electronic record containing the statement and describing the manner in which it was produced;
 - (b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
 - (c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.
- (5) For the purposes of this section,
- (a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
 - (b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
 - (c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation: For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process.

10. After Section 67, the following section shall be inserted, namely:

‘67A. Proof as to digital signature.

Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the

fact that such digital signature is the digital signature of the subscriber must be proved.’

11. After Section 73, the following section shall be inserted, namely:-

‘73A. Proof as to verification of digital signature.

In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct—

- (a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;
- (b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.’

Explanation: For the purposes of this section, ‘Controller’ means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 1999.

12. After section 81, the following section shall be inserted, namely:

‘81A. Presumption as to Gazettes in electronic forms.

The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody.’

13. After section 85, the following sections shall be inserted, namely:

‘85A. Presumption as to electronic agreements.

The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

85B. Presumptions as to electronic records and digital signatures.

- (1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.
- (2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that—
 - (a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;

- (b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

85C. Presumption as to Digital Signature Certificates

The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.'

14. After section 88, the following section shall be inserted, namely:

88A. Presumption as to electronic messages

The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.'

Explanation: For the purposes of this section, the expressions 'addressee' and 'originator' shall have the same meanings respectively assigned to them in clauses (b) and (z) of sub-section (1) of section 2 of the Information Technology Act, 1999.

15. After Section 90, the following section shall be inserted, namely:

'90A. Presumption as to electronic records five years old

Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorized by him in this behalf.

Explanation: Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable.

This explanation applies also to section 81A.'

16. For section 131, the following section shall be substituted, namely:

'131. Production of documents or electronic records which another person, having possession, could refuse to produce

No one shall be compelled to produce documents in his possession or electronic records under this control, which any other person would be

entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.’

The next section analyses the provisions regarding the Bankers’ book of evidence Act as modified by the IT Act 2000.

SCHEDULE III

(Section 92)

Amendments to Bankers’ Book Evidence Act, 1891

1. In section 2—

- (a) for clause (3), the following clause shall be substituted, namely:
 ‘(3) “banker’s books” include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in floppy, disc, tape or any other form of electro-magnetic storage device’;
- (b) for clause (8), the following clause shall be substituted, namely:

‘(8) “certified copy” means when the books of a bank—

- (a) are maintained in written form, a copy of any entry in such books together with a certificate written at the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank’s business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title;
- (b) consist of printouts of data stored in a floppy, disc tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2A.’

2. After Section 2, the following section shall be inserted, namely:

‘2A. Conditions in the printout

A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by the following, namely:-

- (a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager;
- (b) a certificate by a person incharge of computer system containing a brief description of the computer system and the particulars of—
 - (A) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;
 - (B) the safeguards adopted to prevent and detect unauthorized change of date;
 - (C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;
 - (D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;
 - (E) the mode of verification in order to ensure that data has been accurately transferred to such removable media;
 - (F) the mode of identification of such data storage devices;
 - (G) the arrangements for the storage and custody of such storage devices;
 - (H) the safeguards to prevent and detect any tampering with the system and
 - (I) any other factor which will vouch for the integrity and accuracy of the system.
- (c) a further certificate from the person-in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, be relevant data.’

INTELLECTUAL PROPERTY ASPECTS

The Information Technology Act 2000, does not contain provisions relating to electronic copyrights or the protection of phonogram procedures against unauthorized duplication of their phonograms. Similarly, the

question of copyrights for software programmes have not been dealt with in the IT Act.

India is yet to legalize the functioning of online digital department stores, digital book stores and digital record and video shops. Once these are incorporated in the Indian IPR legislation, performers and makers of phonograms, software producers would have benefit of:

- legal remedy against misuse of copyright both direct and indirect in any manner or form;
- right of the owner of copyrights to make available to the public programmes/performance stored in electronic media, by interactive on-demand, online delivery methods;

Commerce on the internet involves the sale and licensing of intellectual property. To promote an effective environment, sellers must know that their intellectual property will not be pirated and buyers must know that they are buying authentic products and not pirated copies. The issues that are likely to come up would include the following:

- Liability of online service providers.
- Fair uses of copyright material.
- Effective patent systems.
- Standards for determining valid claims.
- Litigation due to trademarks.
- Similarity of internet domain names.

To conclude it can be said that in all these matters there is a need for detailed information about case law as is developing in various countries, particularly those where e-commerce has taken firm roots. Newer technology makes it imperative that those entrusted with the job of interpreting these laws, must be thoroughly familiar with the diverse aspects. We have drawn on two or three books dealing with cyber law and would like to acknowledge the great help received in writing this chapter. The books are:

- Yee Fen Lim, *Cyber Law: Commentaries and Materials*.
- Roodney D. Ryder, *Guide to Cyber Laws*.

Regulation of E-finance Institutions

The question of regulating the financial institutions assumes a totally new context particularly after the recent financial debacle. The chapter on 'Risk Management' dealt with recommendations made by Lord Turner in his report to the Chancellor of the Exchequer. Until now one was groping in the dark as to the likely shape of events to come. After the G20 summit (April 2009), the lines are more clearly drawn and the approaches likely to be adopted are also quite clear. One thing is certain, the regulators would not be mere passive observers. The expectation that the market would take care of such deviant behaviour is no longer the mantra; it would be a regulator with a heavy hand. The taxpayers expect deviant behaviour to be severely dealt with. In fact, there would be stringent rules and the scope of regulation would be much wider.

Before elaborating on these topics, two important terms have to be distinguished viz. regulation and supervision. Regulation generally deals with the formation of rules that are on the one side part of the legislation and, thus, approved by national parliaments, and on the other side, rules that are implemented by administrative bodies. Contrary to this, supervision deals with the enforcement of such rules, either *ex ante* in the form of control or *ex post* in the form of sanctions.

During the last two years it has become quite clear that regulating today's super markets in financial services is much more complex a task than is apparent. It is, therefore, necessary for the various authorities, whether working under the same roof like the Financial Services Authority in UK or different bodies working independently, to coordinate their activities and work in close cooperation with each other. It would perhaps be useful if the supervision by objectives approach was adopted and the desired

coordination achieved. However, this section does not detail the broader aspects of regulation; it is restricted to the narrower distribution channel issues.

It has been suggested that the safety and soundness of the Indian banking system, and the part played by the regulators in this behalf, must be highlighted and that the regulators should take steps to actively promote the financial system and ensure that Asian customers as also European and American institutional investors, feel confident about these aspects. Perhaps the RBI could, as in the past, take a lead in promoting investments in advanced technology, ensure adoption of security measures and also make it a point to evaluate the quality of staff deployed. This may be frowned on, but in today's context it is necessary. After all content control could be exercised only under direct supervision. Merely dubbing them as devils on Wall Street would not help.

The 'supervision by objectives' approach is based on the idea that all financial intermediaries and markets are subject to the control of more than one authority. In this regard, each authority is responsible for one objective of regulation regardless of both, the legal form of the intermediaries as well as the functions or activities they perform. The advantage of this approach, which was chosen for example in Australia, is that it is particularly effective in a highly-integrated market context. Therefore, this approach does not require an excessive proliferation of control units. Nevertheless, a regulatory framework organized by objectives has the side effect of a certain degree of multiplication of controls and can, therefore, lead to a lack of controls. Additionally, each intermediary is subject to the control of more than one authority, which might be more costly and moreover the administrative burden for financial intermediaries is significantly increased. However, costs need not deter us at this stage. It is a price to pay for demonstrating the superiority of our systems.

The functional supervisory model postulates a given financial system considered to perform the following basic functions: (a) provision of ways of clearing and settling payments in order to facilitate trade; (b) provision of a mechanism for the pooling of resources and for portfolio diversification; (c) provision of ways of transferring economic resources through time, across borders and among industries; (d) provision of ways of managing risks; (e) provision of price information in order to help the coordination of decentralized decision making in the various sectors of the economy and (f) provision of ways of dealing with the incentive problems created when one party in transaction has information that the other party does not have or when one party acts as agent for another. This reflects on market

efficiencies and arises on account of information asymmetry. However, each type of financial services is regulated by a given authority independent of the operator who offers the services. Therefore, the advantage of this approach is the requirement of the same rules being applied to intermediaries performing the same activities of financial intermediation despite the fact that the operators may fall into different categories from a legal point of view. Moreover, this approach fosters economies of specialization within supervisory authorities and represents an attractive solution for the regulation of integrated and advanced financial markets. Nevertheless, it includes the risk of excessive division of competencies among regulatory agencies.

One perhaps would need a supranational authority both for supervising cross-border transactions and for avoiding regulatory arbitrage advantages/disadvantages. It is true that with coming up of the supermarkets in financial services sector, there is a need for a single authority like the Financial Services Authority (FSA) in UK/Scandinavian countries to overview the myriad functions undertaken by these financial entities. Today, after seeing the AIG debacle, the need for such a body is keenly felt. However, the creation of such a body will have to be viewed from an efficiency perspective also. Additionally, the creation of such a centralized authority at the supranational level has to be critically seen not only on the grounds of excessive concentration of power, but also on a lack of accountability. Moreover, there does not seem to be empirical evidence that justifies the superior wisdom of any given model of organizing financial supervision.

THE REGULATORY CONTENT

The suitability of structures has been dealt with so far. The most important question, however, pertains to the methods which the regulator should adopt to ensure the stability of the system. Equally important is the need to save ourselves from the rogue traders ruining us. How could we let greed and avarice overtake sound business practices? Notwithstanding costs, the regulatory net will have to be cast wider. In the first place, the regulatory systems must be strengthened by bringing in auditors, company secretaries, by publishing risk-based audit reports with management outlook on the future developments and board perception of risk appetite, and so on, every quarter. Further stringent penalties under star chamber systems should also be permissible for gross negligence of systemic security and/or false reporting. Crying hoarse against regulatory costs is easy. Adhering to

strict financial discipline should not be ignored. It is only with a judicious combination of severe penal actions and rigid review that one could break the present unhealthy nexus between rogue traders and bonus dispensers.

Some of the wider questions that need to be handled have been discussed in the following paragraphs. One needs to pay attention to the questions of internet security systems and adhere to guidelines issued by regulators like SEBI. At this stage, we are concerned with the limited question of handling internet security and assume that the wider question of judicious balance between the market freedom and regulatory requirements would be resolved soon.

E-BROKING

Currently, the entire focus of the regulators is on evolving suitable strategies for salvaging the financial institutions and to ensure that the systemic risks are kept within reasonable limits so that the boat does not get rocked by such tremors. These are very genuine concerns, but it is precisely at such times that organizational vigilance has to be in a high state of alert so that fraudsters within and without do not take advantage of the fact that management's attention is focused on much wider issues than on rigid adherence to internal controls. Large scale retrenchment might have created gaping holes in the hierarchical structure and that deciding on lines of control might have been put on the backburner.

The main area of concern for the regulators and senior managements would be to ensure that dealers and others do not resort to excessive risk taking and that the bonuses likely to be paid out do not decide the fate of the organization. The Societe Generale fraud case is a classic example of the laxity of controls. Equally significant, is the case of AIG's credit swap trades, which brought down the entire edifice. It is true that some of these activities were carried on because regulators pleaded inability to control the hedge funds or as in the case of derivative trade did not want to regulate them. The dogmatic belief in market mechanisms could also come in for a great degree of blame in these cases.

Regulation of Broking Services offered through the internet comes under the jurisdiction of SEBI. In 2000 SEBI had issued guidelines for listing of brokers on the stock exchanges. But the circular is not readily available and one has to go to SEBI's website to get the original circular. Since these guidelines are applicable even now, some of the important ones are listed in the following pages for the benefit of the readers.

OPERATIONAL AND SYSTEM REQUIREMENTS

Operational Integrity: The stock exchange must ensure that the system used by the broker has provision for security, reliability and confidentiality of data through use of encryption technology. (Basic minimum security standards are specified in following paragraphs.) The stock exchange must also ensure that records maintained in electronic form by the broker are not susceptible to manipulation.

System Capacity: The stock exchange must ensure that the brokers maintain adequate backup systems and data storage capacity. The stock exchange must also ensure that the brokers have adequate system capacity for handling data transfer and must arrange for alternative means of communications in case of internet link failure.

Qualified Personnel: The stock exchange must lay down the minimum qualification for personnel intending to work as assistants to the brokers. This is to ensure that the broker has suitably qualified and adequate personnel to handle communication, including trading instructions as well as other back office work which is likely to increase in future.

Written Procedures: Stock exchange must develop uniform written procedures to handle contingency situations and for review of incoming and outgoing electronic correspondence.

Signature Verification/Authentication: It is desirable that participants use authentication technologies. For this purpose, it should be mandatory for participants to use certification agencies as and when notified by the government/SEBI. They should also clearly specify when manual signatures would be required.

CLIENT–BROKER RELATIONSHIP

Know Your Client: The stock exchange must ensure that brokers comply with all requirements of ‘Know Your Client’ and have sufficient, verifiable information about clients, which would facilitate risk evaluation of clients.

Broker–Client Agreement: Brokers must enter into an agreement with clients spelling out all obligations and rights. This agreement should also include *inter alia*, the minimum service standards to be maintained by the broker for such services specified by SEBI/Exchanges for the internet-based trading from time to time.

Exchanges will prepare a model agreement for this purpose. The broker agreement with clients should not have any clause that is less stringent/contrary to the conditions stipulated in the model agreement.

Investor Information: The broker website providing the internet-based trading facility should contain information meant for investor protection such as rules and regulations affecting client–broker relationship, arbitration rules, investor protection rules, and so on. The broker website providing the internet-based trading facility should also provide and display prominently, hyperlink to the website or page on the website of the relevant stock exchange(s) displaying rules/regulations/circulars. Ticker/quote/order book displayed on the website of the broker should display the time stamp as well as the source of such information against the given information.

Order/Trade Confirmation: In addition to display of order/trade confirmations on real-time basis on the broker website, such confirmation should also be sent to the investor through email at client's discretion within the time period specified by the client. The investor should be allowed to specify the time interval on the website itself within which he would like to receive this information through email. Facility for reconfirmation of orders which are larger than that specified by the member's risk management system should be provided on the internet-based system.

Handling Complaints by Investors: Exchanges should monitor complaints from investors regarding service provided by brokers to ensure a minimum level of service. Exchanges should have separate cell specifically to handle internet trading related complaints. It is desirable that exchanges should also have facility for online registration of complaints on their website.

RISK MANAGEMENT

Exchanges must ensure that brokers have a system-based control on the trading limits of clients and exposures taken by clients. Brokers must set pre-defined limits on the exposure and turnover of each client.

The broker systems should be capable of assessing the risk of the client as soon as the order comes in. The client should be informed of acceptance/rejection of the order within a reasonable period. In case system-based control rejects an order because of client having exceeded limits, the broker system may have a review and release facility to allow the order to pass through.

Reports on margin requirements, payment and delivery obligations, and so on, should be informed to the client through the system.

CONTRACT NOTES

Contract notes must be issued to clients as per existing regulations, within 24 hours of the trade execution.

CROSS TRADES

As in the case of existing system, brokers using internet-based systems for routing client orders will not be allowed to cross trades of their clients with each other. All orders must be offered to the market for matching.

It needs to be emphasized that in addition to the requirements mentioned previously, all existing obligations of the broker as per current regulation will continue without changes. Exchanges should specify more stringent standards as they may deem fit for allowing internet-based trading facilities to their brokers.

Similar guidelines are also issued by SEBI for brokers offering securities trading through wireless medium on WAP platform. These guidelines are readily available in handbooks issued by publishers like Taxman and could be referred to by the readers. The same could also be seen on SEBI website (www.sebi.gov.in).

For ready reference a brief summary of the mandatory system is provided.

Brief Summary

The system flow of the STP framework would be as follows:

- An STP user intending to send an instruction would send the message to his STP service provider after digitally signing the same.
- The STP service provider would verify the signature of the STP user and forward it to the:
 - recipient STP user, if the recipient STP user is availing services of the same STP service provider; or the
 - STP centralized hub if the recipient STP user is not with the same STP service provider. In such a case, the STP service

provider would be required to prepare a message as per the STP centralized hub prescribed message format, enclose the user's message, digitally sign the message and then send it to the STP centralized hub.

- On receipt of the message by the STP centralized hub, the STP centralized hub would:
 - verify the signature of the sending STP service provider only;
 - send an acknowledgment to the sending STP service provider.
- The STP centralized hub would forward the message to the recipient STP service provider after digitally signing on the message.
- The recipient STP service provider on receipt of the message from the STP centralized hub shall verify the signature of the STP centralized hub, verify if the recipient STP user is associated with it and send an appropriate acknowledgment with digital signature to the STP centralized hub. The STP centralized hub would in turn forward the acknowledgment (received from the recipient STP service provider) duly signed to the sending STP service provider.
- The recipient STP service provider shall forward the message to the recipient STP user. The recipient STP user would receive the message and verify the signature of the recipient STP service provider and sending STP user.
- To enable inter-operation, the STP centralized hub would provide a utility/client software to the STP service provider. The STP service provider's point of interface with the STP centralized hub would be through this utility/client software. The PKI (public key infrastructure) system for the interface shall be implemented at a later stage.

THE INSURANCE SECTOR

This section discusses issues relating to regulation of insurance activities on the internet. The International Association of Insurance Supervisors has brought out a report dealing exclusively with the principles on the supervision of insurance activities on the internet. The recommendations and the rules made by Insurance Regulatory and Development Authority (IRDA) in India have been reviewed in the following pages. The internet creates a new environment in which insurance products can be advertised, sold and delivered, but it does not alter the fundamental

principles of insurance and insurance supervision. It is a new medium to transact business. The Association is rightly concerned about substantial risks to consumers. The opportunities for fraud, money laundering and the mis-selling of insurance products, have, no doubt, been considerably enhanced. The supervisors, thus, have an added responsibility to protect the consumers in their jurisdiction. The questions of applicability of a given contract law and the means of redress in case of a dispute are important issues that need to be settled.

The Association suggests that the supervisors must ensure that the sale, purchase and delivery of insurance are conducted in a secure environment.

Principle 1: Consistency of Approach

‘The supervisory approach to insurance activities on the internet should be consistent with that applied to insurance activities through other media’ (International Association of Insurance Supervisors 2002).

The Association indicates the areas where supervisors must assert their authority over internet activities.

- When an internet site is targeted at residents and/or risks within the supervisors’ jurisdiction.
- When insurance activities are provided via the internet site to residents in the supervisors’ jurisdiction.
- When information is presented to potential policyholders within the supervisor’s jurisdiction through proactive means.

Principle 2: Transparency and Disclosure

‘Insurance supervisors should require insurers and intermediaries over which they exercise jurisdiction to ensure that the principles of transparency and disclosure applied to internet insurance activities are equivalent to those applied to insurance activities through other media’ (International Association of Insurance Supervisors 2002).

It is suggested that the insurer must disclose the address of the head office, the branch office and the jurisdiction in which the insurer can offer such services. It is also necessary that the procedure for the submission of claims and claim handling procedures be indicated.

Principle 3: Effective Supervision Based on Cooperation

‘Supervisors should cooperate with one another, as necessary, in supervising insurance activities on the internet’ (International Association of Insurance Supervisors 2002).

The regulation of internet activities based purely on actions capable of being taken in a single jurisdiction is often inadequate. Therefore, a greater degree of cooperation between supervisors is a must. The Association takes note of operational risks and suggests a close scrutiny of the control mechanism by the insurer.

A truly significant departure is the insistence on the need for the supervisors to observe transparency and their recommendations for disclosure of information through annual reports of the supervisory authority, links to other websites, relevant statistics, and so on. They are quite right in suggesting that the supervisors should publish texts of relevant legislation on their websites.

The approach is somewhat superficial. One gets a feeling that they are hesitating to tread into uncharted areas. The banking supervisors have gone into these matters in a much more detailed manner. Perhaps, the conceptual debate about intervention and leaving it to the market is still not sufficiently tilted in favour of one or the other and, hence, the hesitation. These are sensitive areas and need a greater clarity of approach. It cannot be left to evolve over a period of time.

MONETARY POLICY IMPLICATIONS

Certain aspects of monetary policy, which have not been discussed at length till now, like the growing body of credit card users with ever-increasing drawing limits, are now posing significant problems. Add to these, currencies like ‘Beeze’ or other similar ones and one can understand the woes when consumers start reacting to these newer modes of payment.

There are many who scoff at the idea of any relatively inconsequential device morphing into a major competitor for the US Dollar or the Pound Sterling. It would, in our view, not be at all correct to brush aside the whole subject as ridiculous. Non-banks such as universities and transit systems already issue smart cards backed by the ability of the sponsor to pay. Put these or similar cards in an open environment where they are accepted as vehicles and a ‘new’ currency is available. Together with e-purses, these could provide a formidable area needing control. A possible e-commerce

multi-currency worldview is given in Table 13.1 with details regarding 'New Ways of Paying On-line'.

There are round the world rules against fictitious instruments. But they are not applied to the area of electronic currency. The general apprehension is that once instability sets in, it would be difficult and too late for any remedy. Some European countries have, in our view, rightly allowed only banks to issue such 'currencies'. Further, if and when banking functions get carried out by multiple uncoordinated financial and non-financial entities, who would strive to bring about the 'stability' which is the bedrock of the system. It would not be wrong to say that sound currency and monetary control is more difficult to maintain in this New World of fragmented financial players and multiple currencies. The computers and telecommunication devices have enabled non-bank companies to simulate banking services that customers cannot distinguish. The same forces will enable banks to simulate the functions of currency even though it is not 'legal tender'. The only conclusion is that forces that could destabilize need to be channeled appropriately.

This brings us to the next question. Are smart cards, e-purses covered by deposit insurance? Perhaps, the wider question of safety nets in the financial sector needs to be addressed. Should these instruments be treated separately from other economic agents? In today's world many substitutes for banks' deposit products have emerged and are emerging. Alternate payment mechanisms have also developed. E-finance allows non-deposit taking financial institutions and capital markets to reach far more depositors as well as borrowers. It would not be wrong to say that the whole gamut of 'safety net' is in a melting pot. One could even plead for such safety nets

Table 13.1 New Ways of Paying On-line

<i>A Guide to a New Generation of On-line Payment Systems</i>		
<i>Company</i>	<i>Merchant/Content Partner</i>	
Cyber Gold	Earn and spend programme, Click on ads and spend in network	Animation Factory, Axis3d ZDNet, CD world
E-charge	Advance payment with on-line bank account	
Ipin	Charges digital content to ISP bill	E-music, AT&T music, Virgin Radio, BBC
Millicent	Digital wallets with Milicent 'scrip' inside	Asahi.com. Oxford University Press, and so on

Source: *Journal of Lending and Credit Risk Management*, December 1999–2000.

being extended to other non-deposit institutions. After this the questions relating to the structure and the wider question of currency guarantee need to be addressed. Obviously, the question is related to the consumer protection issue. How do we protect the investors/depositors? Should we lay down minimum standards for institutions and self-regulatory agencies? Equally important is the problem of enforcement. How are these policies to be implemented and by whom?

SMART/DEBIT CARDS

Reserve Bank of India has issued specific guidelines (RBI circular FSC. BC.123/24.01.019/99-2000) to banks, which intend to issue these cards. The Boards of Banks are authorized to decide on issuing such cards and banks have been asked to shoulder responsibility for monitoring the operations. Banks are further advised to ensure safety of these cards. In fact, the losses incurred by customers on account of breach of security or its failure, would have to be borne by the banks. Banks also need to have in place an arrangement for 24-hour notification of loss, theft, and so on of the cards.

COMPETITION POLICY

There is an acute need for global coordination. A series of questions could be posed at this stage and the answers could well depend on certain value premises and the ground realities.

- Would free trade in financial services be the order of the day? It would logically be followed by an equally important question viz. should it be so?
- Should there be free entry? No longer would scale and scope economies be barriers to entry.
- Do we have to reanalyse concepts like markets/competition?

Perhaps, the question could be narrowed down to deciding which payment services should fall under regulatory oversight and which institutions should have access to the payment system? The other alternative is to define them narrowly and restrict it to deposit taking institutions chartered by the regulator. These are important issues and need to be debated and discussed at a time when they have not assumed serious proportions. It is necessary to be ready to meet the contingencies when they arise. The more urgent questions regarding regulation of existing institutions and the

ones coming on the scene remain and need to be addressed. But that does not justify leaving futuristic issues untouched.

A combination of prescriptive measures suggested by the BIS and examination techniques proposed by FDIC are a good starting point. There is considerable unanimity about the proposals made and one is on a safe wicket in adopting them.

The existing risk management principles must be tailored, adapted and in some cases, extended to address specific risk management challenges created by the peculiar characteristics of e-banking activities. 'The RBI could extend the policies enunciated in 1998 [RBI Circulars dealing with Asset/Liability Management and Risk Management: Nos. (a) DBOD No. BP.BC.94/21.04.098/98 and (b) DBOD.No. BP(sc.BC.98/21.04.103/99)] and make it mandatory for banks to adopt the suggestions made by BIS in its report on 'Risk Management Principles for Electronic banking' (as quoted from a report by Bank for International Settlement, Basel) in consultation with RBI. BIS is quite right in asserting that setting detailed risk management requirements must not be counter productive. Each bank's risk profile is different and requires a tailored approach for risk mitigation appropriate for the scale of e-banking operations, the materiality of risks present, and the institute's willingness and ability to manage the risks. This does imply that one-size fits all approach to e-banking risk management may not be universally suited.

Broadly the risk management efforts fall into three groups as discussed further.

MANAGEMENT OVERSIGHT

Effective management oversight of the risks associated with e-banking needs to be in place and risk management should be integrated with overall risk management. There must be an explicit, informed and documented strategic decision—covering specific accountabilities, policies and controls, to address risks. Key aspects of security control process must be covered.

Security Controls

These should include appropriate control processes such as (a) authorization measures, (b) authentication measures, (c) logical and physical controls, (d) adequate security to maintain appropriate boundaries, (e) restrictions on both internal and external user activities, (f) data integrity and (g) audit trails.

DUE DILIGENCE

This includes comprehensive due diligence and management oversight processes for outsourcing relations and third party dependencies.

SECURITY CONTROLS

- Authentication of e-banking customers.
- Non-repudiation and accountability for e-banking transactions.
- Appropriate measures for segregation of duties.
- Data integrity of e-banking transactions, records and information.
- Establishment of clear audit trails for e-banking transactions.
- Confidentiality of key banking transactions.
- Legal and reputational risk management principles.
- Appropriate disclosures for e-banking services.
- Privacy of customer information.
- Capacity, business continuity.
- Contingency planning to ensure availability of e-banking services.
- Incident response planning.

Against the backdrop of information given here the committee has developed the following 14 key risk management principles:

- Management oversight.
- Management of outsourcing and third party dependencies.
- Segregation of duties.
- Proper authorization measures and controls.
- Clear audit trails.
- Authentication of all entities, counterparts and data.
- Non-repudiation of e-banking transactions.
- Comprehensive security.
- Integrity of banking transactions, records and information.
- Appropriate disclosure for e-banking services.
- Confidentiality and privacy of customer information.
- Business continuity and contingency planning.
- Incident response planning.
- Role of supervisors.

The aforementioned suggestions, need to be supplemented with a report prepared by FDIC for bank examiners. The salient features of the suggestions have been listed in the following paragraphs. The summarized

version is in two parts. The standards represent performance objectives to ensure that the bank operates in a safe and sound manner and that the bank's objectives are carried out. Associated risks represent potential threats because of failure to adhere to such standards. The supervisors are advised to look into these areas to see that the banks operate in a safe environment and that the institution's objectives are carried out properly.

The examiners have to ensure that the systems are used with clear strategic direction and with a comprehensive risk management programme. They are apprehensive that critical units may have been excluded from the planning process and that a proper evaluation of costs may not have been made. Further, they are worried that the systems would be such that customer demands would not adequately met. It is noteworthy that the supervisors are keen on ensuring that policies and procedures adequately address the impact on bank activities, operations or security. It is recommended that adequate training of staff on proper controls and potential risks is undertaken. Therefore, the board must establish the standards for overall performance and systems operations. Further, internal and external auditors are advised to review alternate delivery systems. Security of information systems is bound to attract the attention of the supervisors. Outsourcing is the order of the day. Needless to add, such arrangements need to be critically examined by the regulators.

FDIC has recommended the review of following features at the time of examination.

- Planning and implementation.
- Operating procedures and policies.
- Audit.
- Legal and regulatory matters.
- Administration.
- Outsourcing arrangements.

A noteworthy feature is the recommendation that, whenever required, experts may be called in to assist the supervisors. One finds that the examination 'manual', if it could be so described, is a public document and institutions can use it to guide them through a very difficult transition phase.

To conclude, it can be said that in the emerging scenario it is essential for financial institutions, technology firms, auditors and regulators to work closely together in evolving appropriate solutions to safeguard the customer interests, and those of the institutions and of the system as a whole. The newer systems need to be nurtured carefully in the initial stages.

The Internet Potential

Any sound practice is obviously based on equally sound theoretical foundations. It is quite common to hear from seminar participants that they are practitioners and that the theoretical presentations are not of much relevance when it comes to solving so-called practical problems. The fact is that in the financial services sector, most of the practices have a sound legal and, perhaps, even a sounder economic basis. We may not be made constantly aware of it, but for the management to ignore the basics would be a colossal mistake. This is amply borne out by the professed ignorance of senior executives about the products, which were being originated and distributed by their own organizations. To blame the dealers and their indulgent bosses is of no use at all. The fact remains that every one was a party to these decisions and that the aim was to secure maximum bonus possible.

This chapter is an attempt at analyzing the economic values created by the internet and how to use it appropriately.

This chapter has been divided into two parts. Part 1 briefly reviews the management objectives for the massive technology upgrades and the expenses involved in introducing the new technology. Although the internet has been in use in the financial system of advanced countries for quite sometime, there is a feeling that the full potential is not being realized even there. In India, one is led to believe that this upgradation has been more a result of introduction of core banking solutions rather than a conscious decision arrived at because the banks and financial institutions wanted to achieve a given set of objectives or met a genuine customer need. This is clear when one looks at the nebulous objectives like 'Anytime Anywhere banking'. Therefore, this chapter begins with an

analysis of the stated objectives. Unfortunately, the data required for quantitative assessment is not available and we are not able to verify how far the stated objectives have been achieved.

The objectives:

- The main thrust of the banks and financial institutions, in the initial stages, was on meeting the competition from a few banks like HDFC, Citibank and HSBC, which had started offering these services. Therefore, internet-banking facilities were offered to retain and, possibly, to attract the technology savvy customers from the growing IT sector in the country. Some banks in the cooperative sector are even now trying to entice the younger customers by these means.
- Many banks had offered voluntary retirement schemes and were looking for ways to harness the technology support for handling the increased workload or even in handling the existing workload.
- In many public sector banks, the costs of routine transactions like cash receipts and payments, were unusually high because of the staff costs and they had to minimize these to ensure that the customers took to meeting their transaction needs through the ATMs and internet. It was pretty obvious that transaction costs were far too low when the internet was made use of.
- Branch expansion was a costly proposition and efforts had to be made to see that the existing premises were put to proper use while avoiding over crowding.
- Last but not the least, was the convenience offered to customers. The customers who opted for such facilities had the comfort of transacting from anywhere.

THE INTERNET ECONOMICS

At one time, exaggerated claims were made and some theoreticians went to the extent of saying that all that was taught at management courses under subjects like 'managerial economics' was made redundant by the technology developments. There were also tall claims made that bank branches would be closed down and that most banking needs would be met through electronic transactions. The hope was that a few corner shops or kiosks in super markets could meet the needs of 80–90 per cent of the customers. However, the hopes raised by the early success of stand-alone e-banks were soon proved too exaggerated. Soon leading journals began to focus on the failure of these entities. There was a quick transition by

established entities to a new business model viz. 'brick and click' model. This model is currently being followed by most of the banks and financial institutions. They would have to strain to ensure migration of customers to the electronic medium.

In this chapter standard micro economic concepts have been used to examine how value is created on the internet and how this value can be captured. The internet creates value by vastly reducing the costs of transferring information, on a one-to-one, one-to-many or even many-to-many basis. In cases where the product itself is information, the potential for value creation is enormous. In financial services no physical products are involved. Hence, the product or service has significant value content.

It is important to make a comparison between different forms of interaction: personal and internet. This is particularly relevant in a branch setting. It is true that internet interaction is less personal than human interaction., yet it has several characteristics that make it potentially much more valuable in many cases.

- A lot of information can be provided at low cost. Investors can have access to live or recorded interviews with executive officials of an organization, a review of the reports filed with various statutory authorities, and so on. The economies of scale for providing the content, almost globally, make it entirely different from other modes of information transmission.
- The internet allows considerable flexibility in dealing with information. There is a far greater interactivity and search capability than any catalogue or brochure.
- Information access can take place at any time the investor desires and is very useful in differing time zones.
- Value can be created with internet communication either through reduced costs (the supply side) or on the demand side by improving the match between the buyer preference and the goods he may need or want.
- Information about goods comes from the availability of material through various catalogues, histories of consumer purchases comparisons and through aggregators. Customers get annoyed if unsolicited offers are made to them.

It is important to focus on some basic questions like the changing nature of the firm and the intangible products. The previously separate activities of telecommunication, informatics and audio-visual media are crumbling,

and there is a considerable overlap. Time honoured distinctions between home and work place, and intermediate goods and finished products are getting blurred. The intangible economy follows the rules of fuzzy logic of overlap rather than the exclusivity of binary logic.

The aforementioned changes have profoundly affected the production relationships, as also the asymmetry between producers and consumers. The customer, unlike in the past, is no longer ignorant. His decisions are based on information and he has not merely a wide choice but also sufficient guidance in reaching at conclusions. It further facilitates the process of unbundling production and assembly processes. The classic example of such unbundling is the drive in counters at McDonalds. The orders may appear to have been received at a given location, but actually, they are recorded some hundreds of miles away and are supplied in slightly lesser time than if they were received at the given location.

The intangible economy further changes, not only the fundamental nature of economic value, but also the value discovery and capture process. Neither production costs (full cost) nor marginal cost can be used as a guide (conventional economic theory models). It must be noted that, given the ease of replication, purchase does not equal consumption. The number of 'free riders' far exceeds the number of paying consumers. Another problem comes in because of what Stiglitz calls the 'infinite regress'—it is impossible to determine the value of a given piece of information without having this information. Traditionally the pricing of intangibles was a function of the support. The price of a book was determined by the quality of printing, number of pages, and so on. The content can now be priced separately from the support. There is considerable scope for price discrimination. The range of intangible pricing is getting broader and more complex. We are, at this stage, not looking at the pricing of internet services as such, the attention has veered round to pricing of services offered.

However, it appears that the financial services industry in India is not paying much attention to the pricing of these services. In spite of the cost advantages, banks and broking houses have not paid much attention to the charges levied. In fact, the normal method of marketing products is selling the software at almost negligible price and then charging for add-ons or selling a machine cheap and the contents to be priced in a manner that the costs of both are adequately recovered.

Banks are somewhat deficient in informing (some would say, training) their customers about the true state of affairs and more particularly the risk aspects of some newer products in which the banks were trading or offering to their clients. They were to say the least economical with truth. They

could certainly use the channel to increase the awareness about complex products. Further, they could also use the medium for educating the customers about the care that needs to be taken while using internet services. Merely sending out complex printed documents could perhaps absolve the financial institutions, but would it not be better to use more interesting methods to bring home the same message?

It must be pointed out that in a crisis situation sending messages about the solvency of the organization would and has, actually, fuelled more worries than dousing the panic fires. A bank CEOs' views on the current financial crisis would be viewed with greater interest and attention if they are transmitted in the right manner.

Equally important for a large number of customers is the need for a clear and authentic account of the nature of cyber crimes. Such incidents have a more telling effect than some complex instruction booklet. The bank could make the advisories free and charge suitably for the services rendered.

To conclude, it can be said that there is a need for the management to clearly spell out what it expects from the migration of customers to the internet. It also needs to spell out the basis for pricing decisions. The members of the staff who are to operate and market these services are many a time not aware of the rationale and do not take the required initiatives to publicize and market these facilities.

Bibliography

- Abrol, R.K. 1996. 'Electronic Banking (E-Banking)', *IBA Bulletin*, 18(1), January, Mumbai.
- Adavi, Ramesh. 1996. 'Networking the Service Branches', *IBA Bulletin*, 18(1): 104–05.
- Allen, Helen, John Haqwkins and Setsuya Satol. 2001. 'Electronic Trading and Its Implications for Finalizing the Systems', BIS Papers No. 7, BIS, Basle.
- Anandlingam, G. 2003. 'Information Technology Does Matter'. *The Economic Times*, Mumbai, 25 July.
- Andrews, David. 1999. 'Surviving in the Real World', *Banker* (UK), 149(885): 95–96.
- Andriole, Steve. 2002. 'A Winning Technology Strategy'. Available online at <http://itmanagement.earthweb.com/columns/bizalign/article.php/1009331>, accessed on 1 April.
- Appel, M. Andrew, Amit Dhadwal and Wanye Epietraszek. 2003. 'More Bang for the IT Buck', *McKinsey Quarterly*, No. 2, McKinsey and Co. Inc.
- Arnoff, David L. 1999. 'Credit Online: Banking in Cyberspace', *Business Credit*, 101(9): 18–19.
- Asian Banker Journal*. 2000. 'E-Savvy CEOs Who Are Prepared to Lead the Way', *Asian Banking Journal*, 31(January): 20–21.
- Bachman, Timothy. 2001. 'Welcome Back to the Branch', *Bank Marketing*, 33(1), January/February.
- Bank of Japan. 2000. 'The Importance of Information Security for Financial Institutions and Proposed Counter Measures: With a Focus on Internet-based Financial Services'. *The Banker*. 2000. 'Caring for E-Clients', *The Banker* (UK), 150(98): 1–22.
- The Bankers' Book of Evidence Act 1891*, Government of India, New Delhi.
- The Banking Technology. 2000. *Client Relationship Management Report*. London: Informa Professional Publishing.
- Barua, Yogesh. 2005. *Criminal Activities in Cyber World*. New Delhi: Saujanya Books.
- Basle Committee on Banking Supervision. 2001. *Risk Management Principles for Electronic Banking*. Basle: Bank for International Settlement.
- BBC India Profile. 2007. India Internet and Telecommunications Reports. Available online at www.internetworldstats.com/asian/in.htm
- Beans, Kathleen M. 2000. 'Ask the Right Questions in the "Both/and" World', *RMA Journal*, 83(1): 74–75.
- Blount (Ed.). 1999. 'Rethinking the Framework', *ABA Banking Journal*, 91(12): 68–72.
- Brewer, Harold. 2001. 'E-Commerce and Community Banking', *Commercial Lending Review*, 16(3): 48–52.
- Brown Jonathon. 2001. 'Forex Ventures Beyond the Phone', *Euromoney*, (385): 81–84.
- Business India*. 'Changing Face of Banking', *Business India*, Banking Supplement, New Delhi, 21 July–August.

- Cane, Alan. 1985. 'Technology Banking on an Electronic Future', *Financial Times*, 3 June.
- Carr, Nicholas G. 2003. 'IT doesn't Matter', *Harvard Business Review*, May, 41–49.
- Carreker, J.D. 2000. 'Banks and E-Commerce Transforming Old Economy Practices into New Economy Business', *Commercial Lending Review*, 15(4), Fall.
- Carstensen, Brent J. and William D. (Winter). 'Marketing Electronic Banking Products and Services to Bank Customers', *Banker's Magazine*, 179(2): 32–44.
- Castell, Manuel. 2000. *Rise of the Network Society, the Power of Identity*, Volume 2, End of Millenium, Volume 3. Oxford, UK: Blackwell.
- Champy Jim. 2000. 'A Deadly New Game—Computer World'. Available online at www.computerworld.com.au/article/86092A/deadly_new_game, accessed on 26 June 2009.
- Christiansen, Hans. 2000. 'Electronic Finance: Reshaping the World', Financial Discussion Paper No. 4, The World Bank, September.
- . 2001. 'Electronic Finance: Economic and Institutional Factors', Financial Affairs Division—Occasional Paper No. 2, Nov., OECD.
- Classens, Stijn, Thomas Glassener and Daniela Klingebiel. 2001. 'E-Finance in Emerging Markets: Is Leapfrogging Possible?' Financial Sector Discussion Paper No. 7, The World Bank, June.
- Cline, Kenneth 2000. 'Sticky Proposition', *Banking Strategies*, 76(1): 32–34.
- Clinton, Bill. 2003. 'Towards Cooperation', Speech at Yale University, 31 October, Yale.
- Cohen, Stephen S., J. Bradford Delong and John Zyman. 2000. *Berkley Round-Table on the International Economy*. Berkley: University of California.
- Committee on the Global Financial System. 2001. 'Report by a Working Group Established by the Committee on the Global Financial System', BIS, Basle.
- Daniel, Elizabeth and Chris Storey. 1997. *On-line Banking Strategies and Management Challenges—Long Range Planning*, 30(6): 890–98, Elsevier Science Ltd.
- Dayal, Prateek. 2008. Available online at www.Dayal.net/2008, accessed in June 2009.
- De Young, Robert. 2001. 'The Financial Progress of Pure-Play Internet Banks', BIS Paper No. 7, BIS, Basle.
- Dickie, Jim. 2003. 'CRM 2002—State of the Market Place', *Review Marketing Mastermind*, January.
- Drucker, Peter. 2002. 'They Are Not Employees Any More', *Indian Management*, May.
- Duggal, Pavan. 2002. 'Spotlight on Asia Cyber Crimes', *The Economic Times*, Mumbai, 8 December.
- E-commerce and Development Report*. 2002. Internet version prepared by UNCTAD Secretariat.
- The Economist*. 2001. 'The Internet Untethered', *The Economist*, London, 13 October.
- E.T. Intelligence Group. 2002. 'Fighting a Common Enemy, ETIG', *Knowledge Forum*, 10 December.
- Electronic Banking, Safety and Soundness Procedures, FDIC Division of Supervision.
- Elumalai, Dr K. 2001. 'Legal Regulation of Cyber Crimes—Salient Features of Information Technology Act 2000', Paper presented at the Conference on Cyber Laws and Legal Education organized by Nalsar University of Law, Hyderabad.
- Fadia, Ankit. 2009. 'Ethical Hacking Training'. Available online at www.innobuzz.in, accessed in June 2009.
- Farrel, Diana, Terra Terwilliger and Allen P. Webb. 2003. 'Getting It Spending Right This Time', *Mckinsey Quarterly*, No. 2.
- Federal Deposit Insurance Corporation (FDIC). 2000. *Security Monitoring of Computer N*, FDIC, Financial Institutions Letter, October.

- FDIC. 2002. *Digital Signature, Deployment Issues, FDIC bulletin on Digital Signatures*, July.
- Ferrash, Edward (1999–2000). 'The Last World: Been Ztm??? Yes, Beenz', *Journal of Lending and Credit Risk Management*, December–January.
- 'Financial Markets and World Economy', G20 Summit held on 2 April 2009.
- Financial Times*. 2003. Report published in *Financial Times*, London, 4 June.
- Financial Times IT Review*. 2003. 'A Focus on Mobile Working—What It Means for You and Your Boss', *Financial Times*, London, 29 October.
- Gandy, Anthony. 1996. 'Competing in the Electronic Marketplace', *Chartered Banker*, 2(10), October.
- Gates, Bill. 1995. 'No Company's Future is Guaranteed', Economic Times Interview, *The Economic Times*, Mumbai, 12 December.
- . 1997. 'The Future is Now: I am a Big Believer', The Bill Gates Chatmode, *The Economic Times*, Mumbai, 5 March.
- Gillis, M. Arthur. 2000. 'In-House or Outsource? Still a Popular Question', *ABA-Banking Journal*: 51–56.
- Goldfinger, Charles. 2000. Intangible Economy and Financial Markets, Preliminary Exploration Contribution to IDATE Conference 'NEW Economy', 15 November.
- Gosling, Paul. 2002. *Financial Services in the Digital Age*. London: The Bowerdon Publishing Company.
- Government of India. 2000. *The Information Technology Act, 2000*. New Delhi.
- Greenspan, Alan. 1998. 'The Structure of the International Financial System', Speech at the Annual Meeting of the Securities Industry Association, Boca Raton, 5 November, Florida, USA.
- The Guardian*. 2003. 'Business Solutions, Smart Business of SMEs', *The Guardian*, London, October.
- Gurumurthy, N. 2001. 'My Vision of SBI in 2010', *SBI Monthly Review*, October.
- Haldipur, Rajesh. 1998. 'The New Face of Retail Banking', *Indian Management*, 37(11): 19–27.
- Heath, Ray. 1999. 'Cashing Out', *Banking World*, (68): 8–10.
- Hirst, David. 2000. 'Rewriting the Rule Book', *Banker* (UK), 149(883): 72–73.
- Ho, Andy. 1999. 'Playing with the Big Boys', *Banking Technology*, 15(6): 32–34.
- Home news Rppm. 2007. Internet Penetration in India. Available online at www.dailyreckoning.com, Australia.
- Horsefield, Richard. 2000. 'Shaping the Future of Online Financial Services', *Banker* (UK), 150(887): 26–28.
- Ignotius, George. 1997. 'Internet Banking – Inviting Virtual Holdups?' *Dataquest*, 15(18): 143–46.
- International Association of Insurance Supervisors. 2002. 'Risks to Insurers Posed by Electronic Commerce', IAAS Issue Paper approved in Santiago de Chile, October.
- Johnston, Lawrence. 2000. 'Finger on the Pulse', *Banking Technology*, 17(2): 30–33.
- . 2001. 'Defence in Depth', *Banking Technology*, 17(2): 30–33.
- Joshi, Vasant C. and Vinay V. Joshi. 2009. *Managing Indian Banks: The Challenges Ahead*. New Delhi: Sage Publications.
- Jud Elizabeth. 2000a. 'Leap of Faith', *Banking Strategies*, 76(3): 36–40, 46.
- . 2000b. 'Marketing: Serving the Seniors Online', *Banking Strategies*, 76(6): 24–30.
- . 2000c. 'Retail Banking: The B2E Connection', *Banking Strategies*, 76(6): 6–10.
- Karandikar, S.K. 2000. 'E-Commerce and Banking', *IBA Bulletin*, 21(3): 26–32.
- Kates, Geoff. 2001. 'Back to Basics', *Banking Technology*, 18(3).
- Keeton, Williams R. 2001. 'The Transformation of Banking and Its Impact on Consumers and Small Business, Federal Reserve Bank of Kansas City', *Economic Review*, 86(1): 25–53.

- Kish, John. 2000. 'Before your Customers Leave: Trend of High Attrition Rates?' *Bank Marketing*, 32(12): 30–35.
- Knaapschaefer, Johnna. 2000. 'Banking on Customer Focus', *Marketing Mastermind*, August.
- Lihui Lin, Xianjan Geng and Andrews Whinstol. 2000. 'A New Perspective to Finance and Competition and Challenges for Financial Institutions in the Internet Era', BIS Paper No. 7, BIS, Basle.
- Lim, Cindy. 2000. 'We will Build it and They will Come', *Asian Banker Journal*, (21): 13–15.
- Lomax, Victoria. 2000a. 'Checkmate', *Banking Technology*, 17(7): 36–40.
- . 2000b. 'Small Change', *Banking Technology*, 17(6): 28–32.
- London, James. 'F-Flops Hold Lessons for Electronic Bankers', *ABA, Banking Journal*, 81(1): 40–44.
- Lucas, Louise. 1998. 'Whispers in the Future', *Banking Technology*, 15(6): 48–50.
- Luke, Rob. 2001. 'Joint Effort?' *Banking Strategies*, 77(1): 37–42.
- May, A. Thorton. 1997. 'Electronic Commerce: Three Truths for IS', Leadership Series, *Computer World*, April.
- McAfee, Andrew. 2003. 'When Too Much Knowledge is a Dangerous Thing', *MIT Sloan Management Review*, Winter.
- McCarthy, Paul. 2001. 'The Future Is Mobile', *Banker (UK)*, 151(899): 118–19.
- . 1997. 'Technology: Securing the Lines', *Banking World*, (42): 24–25.
- McCorminik, Joel. 1999. 'Going with the Flow', *Banking World*, (63), March, Hong Kong.
- McKenzie, Heather. 2000–2001. 'Delusions of Grandeur', *Banking Technology*, 17(10), December–January.
- Mercer, Don. 1998. 'Doing Business in a Borderless World', *Payment Systems Worldwide*, 9(2): 30–32.
- Mike, M.W. 2001. 'The Shopper Stopper', *ABA Banking Marketing*, 33(80): 38–41.
- Milton, Dan. 1996. 'More Bang for the Bank', *Dataquest*, 14(12): 68–71.
- Mishra, K.C. 1999. 'The Fifth Channel of Banking: Internet Banking', *State Bank of India Monthly Review*, 38(7): 1028–35.
- Mohan, Rakesh. 2009. 'Global Financial Crisis', Speeches Delivered at Hyderabad, Yale and London Business School, 23 April 2009.
- Nadler, Paul S. 2000. 'Fact and Fiction in Internet Banking', *Secured Lender (USA)*, 56(3): 44–48.
- Narayana (Justice) P.S. 2002. 'Cyber World–New Challenges', Lecture Delivered at University of Hyderabad, 23 May.
- National Stock Exchange of India Ltd. 2000. 'Internet Based Trading Services, Circular No. NSE/F7O/1877', 24 August.
- . 2001. 'CTCL/Internet Based Trading Facility, Circular No. NSE/F&O2788', 17 August, Mumbai.
- Nayak, Gayatri. 2002. 'When Small is Big', *The Economic Times*, Mumbai, 7 August.
- The New York Times*. 2002. 'Internet Untethered', *The New York Times*, New York, August.
- Norton, Mike. 1999. 'Any Portal in a Storm', *Banking Technology*, 16(5): 36–42.
- Orr, Bill. 2000. 'Financial Portals are Hot but for Whom?' *ABA Banking Journal*, 92(7): 53–60.
- . 2001. 'E-Banking: What Next?' *ABA Banking Journal*, 93(12), December.
- Outlook*. 2003. 'Indian Banks coming of Age', *Outlook*, Delhi, 28 July.
- Padwal, S.M. 2000. 'The Role of Security Standards in Payment Systems Design', *Payment Systems Worldwide*, 11(2).
- Palmer, Andrew. 2000. 'Internet Banking's Hollow Promise', *Economist Newspapers*, London, 9 November. Available online at www.economist.com/displayStory.cfm?story

- Palmer, Andrew. 2009. 'Rebuliding the Banks', *The Economist*, London, 14 May 2009. Available at http://www.economist.com/specialreports/displaystory.cfm?story_id=13604663.
- Percy, Tom. [2000–200com/asia/in], "Joined at the Seams", Banking Technology, Informa Publishing Group Ltd.
- Pitawalla, Yasir A. 2000. 'Right Product Mix', *The Economic Times*, Mumbai, 20 March.
- Porter, Michael E. 1985. *Competitive Advantages Creating and Sustaining Superior Performance*. New York: The Free Press.
- Post, David D. and D. Johnson 1996. 'Law and Borders: The Rise of Law in Cyberspace', *Stanford Law Review*, 48: 1367.
- Powers, Robert. 1998. 'Building a Website that Works: Here's How', *Journal of Lending and Credit Risk Management*, 80(10): 20–23.
- Reserve Bank of India. 1999–2000a, 'Off-Site Monitoring and Surveillance Systems in Select Countries', Report on Trend and Progress of Banking in India, Mumbai.
- . 1999–2000b. Guidelines for the issue of Smart/Debit Cards by Banks, Circular No. FSC.BC.123?24.01.019/99–2000, RBI, Mumbai.
- Roberson, Mark S. 1989. 'The Role of Technology in a Changing Banking Industry', *World of Banking*, 8(6): 18–21.
- Rutberg, Sydney. 2000. 'Five Year Outlook for the Commercial Finance industry: The Majors Speak of Growth, Change, and Opportunity', *Secured Lender* (USA), 56(3) May/June.
- Ryder, Robert D. 2005. *Guide to Cyber Laws*. Delhi: Mohan Law House.
- Santomero, Anthony M. 1997. *Commercial Bank Risk Management: An Analysis of the Process*, Financial Institutions Centre, The Wharton School, University of Pennsylvania, February 28.
- Schutzer, Daniel. 1998. 'The Role of Public Key Cryptography, Digital Signatures, and Digital Certificates in Electronic Commerce', *The Journal of Lending and Credit Risk Management*, June.
- Sitjin, Classens, Thomas Glassener and Daniel A. Klingebiel. 2000. E-Finance in Emerging Market Economies, 'Is Leapfrogging Possible?' Discussion Paper No. 7, The World Bank, June.
- Srinivasan, Aruna. 2002. 'A New Spin of the Web', *The Economic Times*, Mumbai, 16 June.
- Stiglitz, J. 1985. 'Information and Economic Analysis: A perspective', *Economic Journal*, 95.
- Stoneman, Bill. 2000. 'The Message, not the Medium', *Banking Strategies*, 76(2): 6–10.
- Tata, Ratan. 2000. 'Biz is What it is all About', *Business Today*, 21 October.
- Toffler, Alvin. 1990–92a. *The Future Shock*. New York: Batman Books.
- . 1990–92b. *The Third Wave*. New York: Batman Books.
- . 1990–92c. *Powershift*. New York: Batman Books.
- Turner, Jonathan Adair. 2009. 'The Turner Review', Financial Services Authority, 18 March, London.
- Vasudevan, A. 1998. *Committee on Technology Upgradation*. Mumbai: RBI.
- Wahrenburg. 2001. 'Trading Systems Competition and Market-market Competition', BIS Paper No. 7, BIS, Basle, March.
- Wates, Richard. 2003. 'Corporate Computing Tries to Find a New Path', Financial Times Special Report, IT Review, *Financial Times*, London, 4 June.
- Watson, Richard. 2005. 'The Future of Money'. Available online at www.fastcompany.com/resources/innovation/watson/050905.htm, accessed on 26 June 2009.
- Yee Fen Lim. 2002. *Cyber Law: Commentaries and Materials*. Melbourne: Oxford University Press.

Index

- access control using
 - password and PIN, 121–22
 - tokens and smart cards, 122–23
- access devices, 19
- account aggregator, 22
- Advantage mortgage, 31
- aggregation, 21
- aggregator, 19, 21–22, 60
- AIG debacle, 60–61, 161–62
- alternate system of trading, 109–10
- Application Programming Interface (API), 23
- Application Service Provider (ASP), 41–42
- asymmetric cryptography, 125, 146–47
- asymmetric key encryption, 124–26
- automated scanning tools, 129
- automated teller machine (ATM), 37, 43, 83
- Bankers' Book of Evidence Act, 1891, 112, 115–16, 141, 146, 156–57
- Bank for International Settlement (BIS)
 - guidelines for risk management, 99, 104–05, 114
- Basel Committee on Risk for Electronic Banking, 91, 100–01, 106
- biometrics authentication techniques, 123
- black hackers, 94
- Bombay Stock Exchange, 66, 71
- book store effect, 78
- Brick and Click model, 5, 13, 18, 28, 40, 56, 65, 74–89, 175
- business planning, integration with marketing, 78–80
- Business-to-Consumer (B2C) segment, 31
- card-based scheme, 30
- Carnegie Mellon Software Engineering Institute Network Systems Survivability Program, 131
- certification authority (CA), for digital signatures, 148–50
- Civil Procedure Code, 141
- Clearing Corporation of India, 10, 67, 71–73
- click and brick marketing, *See* marketing
- Code of Criminal Procedure, 112
- configuration issues, 133
- connectivity risks, 108
- control devices, in network security, 121–23
- corporate plans, marketing plan in, 79–80
- cracker, 112
- credit risk, 90–91
- Cryptographically Strong Pseudo Random Number Generator (CSPRNG), 126
- cryptographic keys, 113
- customer service, 5, 29, 35, 39, 74, 76
- cyber crime, 111–17
 - effects, 114
 - enforcement problems, 115–17
 - forms, 112
 - IT Act and, 113–14
 - real and hearsay evidence, 115
 - reasons, 112–13
- cyber laws
 - contract aspect, 144–45
 - evidence aspect, 149–57
 - functional equivalent approach, 145–49
 - intellectual property aspects, 158
 - jurisdiction, 143–44

- data systems incompatibility, 108
- data transmission reliability, 124
- denial of service attacks, 129, 132
- digital signatures
 - certification, 148–50
 - creation of, 147
 - definition, 146
- due diligence, and risk, 100, 105, 172
- e-banking, 22–24, 37–59
 - access to, 37
 - ASP selection, 42
 - bankers perception, 38
 - bank websites, 42–45
 - B2B applications, 48
 - definition, 37
 - differentiation aspect, 52–53
 - efficacy evaluation, 52
 - impact assessment, 50–51
 - internet and non-internet banks, 56
 - mobile banking, 58–59
 - objectives, 46
 - planning and development, 39–45
 - problems encountered, 22–24, 39
 - products and services offered, 46–47
 - risks
 - BIS recommendations for management, 99, 104–06
 - conduct of business, 108–09
 - connectivity, 108
 - data security, 108
 - factors, 53–54
 - management, 104–10, 164–65
 - operational, 107
 - transaction, 107–08
 - security measures, 109–10
 - to small- and medium-sized enterprises, 49–50
 - stand-alone e-banking, 54–58
 - strategic risks, 106–07
 - structural deficiencies, 107
 - systems and services management, 137–40
- e-banking, 162–66
 - client-broker relationship, 163–64
 - contract notes, 165
 - cross trades, 165–66
 - operational and system requirements, 163
 - risk management, 164–65
 - STP framework, 165–66
- e-commerce, *See also* e-banking
- attendant risks, 108–09
- Economic Cycle Reserve, 92
- e-finance
 - competition and cost savings, 15–16
 - cost savings, 15
 - delivery channels, 10–16
 - enabling services and their importance, 8
 - institutions regulation, 159–62
 - internet pervasiveness and, 14–15
 - IT as infrastructure technology, 12–14
 - problems associated with, 19–20
 - returns on IT investments, 11–12
 - service, 37
 - transition to, 7
- e-finance institutions
 - competition policy, 170–71
 - e-broking, 162–66
 - insurance sector, 166–68
 - investor information and complaints, 164
 - management oversight
 - and due diligence, 172
 - security controls, 171–73
 - monetary policy implications, 168–70
 - operational integrity, 163
 - order/trade confirmation, 164
 - personnel and procedures, 163
 - regulation, 159–62
 - regulatory contents, 161–62
 - risk management principles, 172
 - signature verification and authentication, 163
 - smart and debit cards, 170
 - system capacity, 163
- e-insurance, 59–62
 - risk management for, 104–10
- electronic fund collection, through e-trading, 69–70
- electronic system, and risk, 94
- e-money, 30–32
- encryption attacks, 132
- e-procurement, 33–36
- e-purse schemes, 30
- equity markets, e-trading in, 33
- e-security, in wireless network, 131

- ethical hackers, 94
- e-trading, 63–73
 - advantages, 64–65
 - electronic fund collection, 69–70
 - in equity markets, 33
 - in fixed-income securities, 70–72
 - in foreign exchange, 72–73
 - indicative or tradable, 68
 - pre-trade transparency, 68–69
 - price quantity real-time or delayed, 68–69
 - services, 64
 - in shares, 69
 - systems, 33
 - transparency, 67–69
- Federal Deposit Insurance Corporation (FDIC), 39, 171–73
 - guidelines, 93–94, 99, 101, 105
- Financial Market Directive (MIFID), European Union, 67–68
- firewall, 126, 128
- fixed-income securities, e-trading in, 70–72
- floor-based trading, 64
- foreign exchange trading, 33, 72–73
- fraudulent data misuse, 94
- General Packet Radio Service (GPRS)
 - vulnerability, 135
- Grameen Bank, Bangladesh, 7, 33
- Gray bank, e-banking at, 44
- Groupe Spécial Mobile (GSM)
 - and network security, 134–37
 - security solutions for, 136–37
 - vulnerability
 - GPRS, 135
 - SIM cards, 134–35
 - SMS, 135–36
 - WAP weaknesses, 136
- hackers, 43, 94, 97–98, 112–13, 120, 122, 132
- hedge funds, 92
- IDS alert notifications, 129
- I-Flex solutions, 41–42
- incident response, in network security, 129–30
- Indian Contract Act, 141
- Indian Evidence Act 1872, 112, 115, 141, 146, 150–56
- Indian Penal Code, 1860, 112, 146
- information security risk assessment, 95
- Information Technology (IT) Act, 2000, 112–13, 115, 141, 145–46, 149–56
- in-house work done, 24–26
- insertion attacks, 132
- Insurance Regulatory and Development Authority (IRDA), 35, 59, 61, 166
- insurance sector, 106, 166–68
- intangible products marketing, 77–78
- Intellectual Property Rights (IPR), 116, 158
- International Association of Insurance Supervisors, 106, 166–68
- internet
 - banking, *See* e-banking
 - characteristics, 4
 - economics, 175–78
 - enabled insurance, 61–62
 - evolution, 2–4
 - impact assessment, 5–7
 - interaction and personal interaction, 176
 - and non-internet banks dynamic analysis, 55–56
 - objectives, 175
 - pervasiveness and e-finance, 14–15
 - potential, 174–78
 - trading, *See* e-trading
 - for underdeveloped countries, 7
 - users growth, 2–3
- Internet Protocol (IP) spoofing, 98
- internet services
 - clean slate approach, 29
 - continual evolver approach, 28–29
 - e-money, 30–32
 - e-procurement, 33–36
 - e-trading, 33, 63–73
 - factoring and leasing, 32–33
 - problems associated, 28
 - reasons retarded developments of, 27–28
 - traditional migrator approach, 28
- intrusion detection systems (IDS), 95, 127

key encryption, 122, 125–26

liquidity
 regulation, 92
 risk, 90–91

majeure risks, 103

malicious attacks, and network security,
 123–24

Management Information System (MIS), 49
 management oversight
 and due diligence, 172
 of risks, 100, 105
 security controls, 171–73

managers' check list
 in marketing, 85–86
 for network security, 127–29

market
 risk, 90–91
 turbulence, 87–88

marketing, 76–88
 customers and, 76, 84–86
 grievance redressal, 87
 intangible products, 77–78
 integrating with business planning,
 78–80
 managers' check list, 85–86
 market turbulence, 87–88
 max-e-imperatives, 84–85
 objectives, 80–85
 plan in corporate plans, 79–80
 strategy evaluation, 86–87
 supplier reach, 82–83

market would take care approach, 92–93

micro finance agencies, 49

mobile banking, 58–59

mobile node to mobile node attack, 133

Mobitrack service, 66

Model Law on Commercial Arbitration,
 145–46

Multilateral Trading Facilities (MTFs),
 67–68

National Infrastructure Protection Center
 (NIPC), 131

National Stock Exchange, 10, 71

Negotiated Dealing System of RBI, 70

network security, 118–40

 access control using
 password and PIN, 121–22
 tokens and smart cards, 122–23
 asymmetric key encryption, 125–26
 best practices in use, 128–29
 control devices, 121–23
 data transmission reliability, 124
 e-banking systems and services, 137–40
 e-security, 131
 failures, 119–21
 GSM and, 134–37
 incident response, 129–30
 malicious attacks, 123–24
 managerial checklist, 127–29
 manager's laptop problem, 132–33
 random numbers use, 126–27
 survivable system development, 130–31
 war driving, 132–34, 136
 wireless networks, 131–33

online client interface categories, 18

on-line payment systems, 169

online trading, implementation stage
 difficulties, 22–24

online value chain, 19–21

operational

 integrity, 163
 risk, 90–91, 107

organizational control, risk beyond, 102–03
 outsourcing, 24–26

 e-finance systems and services manage-
 ment, 137–40

 risk of, 102

password

 access control using, 121–22
 generation, 121
 theft, 98, 112

penetration

 analysis, 95
 testing, 126

personal digital assistant (PDA), 37, 43

personal identification number (PIN), access
 control using, 121–22

pre-trade transparency, in e-trading, 68–69

Project Entropia, 30–31

- pseudo-random number generators (PRNG), 126
- pseudo-random numbers (PRN), 126
- public key infrastructure (PKI) system, 128
- random numbers, use in network security, 126–27
- RBI Act of 1934, 141, 146
- regulatory framework, for telecommunication, 8–9
- Reserve Bank of India (RBI), 70–72, 74, 99, 160, 170–71
- risk
 - analysis, 90–91, 105
 - assessment, 95–97
 - beyond organizational control, 102–03
 - conduct of business, 108–09
 - connectivity, 108
 - data security, 108
 - due diligence, 100, 105, 172
 - electronic system, 94
 - elements, 90–91
 - institutional and geographic regulation, 92–94
 - management
 - aspects, 90–103
 - Basel committee and, 100–01, 106
 - BIS guidelines, 99, 104–06
 - for e-banking and e-insurance, 104–10
 - FDIC guidelines, 93–94, 99, 101, 171–72
 - mechanism, 99
 - oversight, 100, 105, 171–73
 - principles, 100–01, 172
 - operational, 90–91, 107
 - of outsourcing, 102
 - potential threat, 97–100
 - preventive measures, 94–95
 - security controls, 100–02, 105, 171–73
 - strategic, 106–07
 - transaction, 107–08
 - Turner recommendations to manage, 91–92
 - vulnerabilities, 96–97
- RSA asymmetric cipher, 125
- Scare Socket Layer (SSL) protocol, 125–26, 136
- securities, e-trading in, 33
- Securities and Exchange Board of India (SEBI), 65, 69, 71–73, 109–10, 162–63, 165
- security controls and risk, 100–02
- security failures, 119–21
- self-help groups (SHGs), 49
- shares, e-trading in, 69
- short message services (SMS) vulnerability, 135–36
- signature verification and authentication, 163
- Simple Network Management Protocol (SNMP), 128
- small- and medium-sized enterprises, e-banking to, 49–50
- smart cards, 170
 - access control using, 122–23
- sniffing, 113
- social engineering, 98, 113
- South Africa's Standard Bank, 32
- stand-alone e-banking, 54–58
- State Bank of India, 34
- stealers, 112
- strategic risks, 106–07
- subscriber identification module (SIM) card vulnerability, 134–35
- supplier reach, in marketing, 82–83
- survivable network security system, development of, 130–31
- Swedish Financial Supervisory Authority, 30
- symmetric key encryption, 124
- telecommunication, regulatory framework for, 8–9
- telenet, 128
- telephone-based trading, 64
- threat, to computer security, 97–100
- tokens, access control using, 122–23
- trading, *See also* e-trading
 - alternate system, 109–10
- traffic interception and monitoring, 132, *See also* war driving
- transaction risks, 107–08
- transparency, in e-trading, 67–69
- Trojan horses, 98–99, 123–24
- Uncitral Model Law, 115, 149
- United Nations Commission for Contracts for International Sale of Goods, 146, 149

- VAR measures, 91
- virtual private networks (VPN), 126, 136–37
- viruses, 99, 129
- voice-over IP, 129
- vulnerabilities
 - assessment tools, 95
 - risk assessment and, 96–97
- war dialing, 98, 133
- war driving, 132–34, 136
- websites
 - access devices, 19
 - aggregator, 21–22
 - attacks on, 43–45
 - design strategy, 20–21
 - development of, 17–18
 - e-banking, 22–24, 42–45
 - online trading, 22–24
 - online value chain, 19–21
 - outsourcing and doing it yourself, 24–26
 - portals, 19, 21–22
- weightless economy, 77
- wide area network (WAN), 137
- Wireless Application Protocol (WAP)
 - weaknesses, 136, 165
- Wireless Equivalent Protocol (WEP), 132
- Wireless Markup Language (WML), 136
- wireless network (WLAN), e-security in,
129, 131–33
- Wireless Transport Layer Security (WTLS),
136
- Worms, 123–24