STRATEGIES TO MITIGATE RISK IN INTERNET BANKING

DR. R.K. UPPAL
Director, ICCSR Sponsored Major Research Project
D.A.V. College, Malout (Punjab)
E-mail rkuppal_mlt@yahoo.com

Abstract

Technology on the one hand proves to be very helpful in increasing the efficiency and profitability of the banks and on the other hand it creates lot of risk for the banks and customers. The present paper is an attempt to study the risk in internet banking. The study takes some parameters like growth of I-banking branches, growth of I-banking customers, and impact of e-delivery channels on the profitability of the scheduled commercial banks. On the basis of these parameters the study concludes that with the growth of information technology, I-banking branches and customers are increasing in all the bank groups. This is the reason that risk in internet banking is increasing. But as the I-banking pose a positive impact on the profitability of the banks so it is a need of time to mitigate this risk. To mitigate the risk in internet banking the paper also suggests some strategies

Keywords: Risk in I-banking, Mitigation of Risks

Introduction

Globalization has increased competition and regulatory changes are creating new business and markets. Recent events have forced corporations to consider risk exposure on a daily basis. In the current market, risk management is thus a critical component of overall business management. Risk management is present in all aspects of life. It is about the every day trade-off between an expected reward and a potential danger. The notion of risk is much larger. It is universal, in the sense that it refers to human behaviour in the decision making process. Risk management is an attempt to identify, to measure, to monitor and to manage uncertainty (D. Ravishankar, p. 30). Technology also creates risk particularly internet banking risk. Internet banking refers to the system that enables bank customers to access accounts and general information on bank products and services through a personal computer or other intelligent device. There is always lurking danger of hackers and cyber criminals who can access the bank accounts and cause havoc. That brings us to twin challenges faced by a citizen with regard to the internet. Is the citizen entitled to his privacy? Is he secure? Thus internet banking creates new challenges for banks as it opens fresh way of exposure. From a supervisory perspective, risk is that events, expected or unexpected, which have an adverse impact on the bank’s earnings or capital (A. Saxena, p. 24)
Types of Internet Banking

There are three basic kinds of internet banking which are being employed in the market place.

- **Informational**

  This is the basic level of internet banking. Typically, the bank has marketing information about the bank’s products and services on a stand-alone server.

- **Communicative**

  This type of internet banking system allows some interaction between the bank’s systems and the customer. The interaction may be limited to electronic mail, account inquiry, loan applications or static file updates.

- **Transactional**

  This level of internet banking allows customers to execute transactions. Customer’s transactions include accessing accounts, paying bills, transferring funds etc.

### Review Of Related Studies

Sharma, M. (2003) studies the major accounting policies pertinent to risk management functions of banks internationally and in India. The study finds wide divergence in some policies such as those relating to credit and interest rate risk. It also finds that the Basel Committee recommendations require far greater disclosures than presently provided by the Indian banks.

Pathrose, P.P. (2003) analyzed that Reserve Bank underlines the important role a sound internal audit function plays in contributing to the effectiveness of the internal control system in banks. The risk-based internal audit would not only offer suggestions for mitigating current risks but also anticipate areas of potential risks and play an important role in protecting the bank from various risks.

Kumar, S.N.V. (2003) explores the major financial risk forced in the capital and debt markets. The paper explains the need for articulating risk policy and profile of the organization. The paper conclude that financial sector risk need to be viewed as not only risks relating to decision making process, but also the risk associated with the organizational structure, processes, management procedures, human resource and culture that affect the decision making process.

Rajeev, A.S. (2005) concludes that the first line of defence against operational risk may be systems and controls within the firms but there is also a role of capital. The real nightmares facing banks are catastrophic losses that threaten the viability of the organization. These typically involve rogue trading, insider fraud, bad lending, poorly understood derivatives, inadequate
controls and natural disaster. Capital buffers play an important role in reducing the likelihood of even catastrophic losses.

Sen, P. (2008) in his article basic concept of credit risk and it management has been described component wise and in an orderly sequence taking latest developments into account. Management of credit risk includes identification of risk, assessment of risk through credit rating/scoring, quantification of risk through estimate of expected and unexpected loan losses, pricing of loan products on a scientific basis, controlling and monitoring of risks through effective loan review mechanism.

Objectives, Research Methodology And Database

Objectives

- To study and analyze the extent of internet banking and their customer base in various bank groups.
- To study and analyze the impact of e-channels on profitability of bank groups.
- To prepare strategies to mitigate the internet banking risk in banks.

Research Design

Internet is a mixed blessing. When people do transaction on the internet, there is always the lurking danger of the hackers and cyber criminals who can access bank account and cause havoc. This brings us to risk faced by citizen with regard to internet. Thus the challenge of security is more serious. It is a need of time to manage the risk caused by the internet.

Sample Design

The present study is based on the Indian banking industry which comprises of four major bank groups.

- SBI & its associates – G-I (08)
- Nationalized banks – G-II(20)
- Old private sector banks – G-III (20)
- New private sector banks – G-IV (07)
- Foreign banks – G-V (29)

Parameters of Study

The study takes into considerations following parameters:

- Growth of I-banking in scheduled commercial banks
- Growth of I-banking customers in scheduled commercial banks
Impact of e-channels on the profitability

All the parameters have been analyzed for the period 2001-2007

Database

Results And Discussion

I-Banking As A Percentage of Total Branches

In the year 1999, various e-delivery channels were introduced. I-banking is one of those e-delivery channels. Some banks adopt I-banking to increase their customers. It can be seen from the table 1 that branches of internet banking are increasing in all the bank of groups. But in G-IV and G-V use of I-banking is much as compared to G-I, G-II and G-III. Thus with the increasing number of branches risk in internet banking is also increasing.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>G I</td>
<td>11.8</td>
<td>16.2</td>
<td>23.0</td>
<td>32.2</td>
<td>35.0</td>
<td>40.3</td>
<td>51.4</td>
<td>29.9</td>
</tr>
<tr>
<td>G II</td>
<td>1.55</td>
<td>1.94</td>
<td>2.74</td>
<td>4.34</td>
<td>5.01</td>
<td>6.65</td>
<td>8.40</td>
<td>4.37</td>
</tr>
<tr>
<td>G III</td>
<td>6.25</td>
<td>7.98</td>
<td>15.0</td>
<td>15.6</td>
<td>17.6</td>
<td>20.7</td>
<td>23.9</td>
<td>15.29</td>
</tr>
<tr>
<td>G IV</td>
<td>74.1</td>
<td>72.9</td>
<td>80.8</td>
<td>77.9</td>
<td>62.8</td>
<td>74.2</td>
<td>66.2</td>
<td>72.7</td>
</tr>
<tr>
<td>G V</td>
<td>42.1</td>
<td>45.5</td>
<td>47.2</td>
<td>78.0</td>
<td>78.0</td>
<td>47.3</td>
<td>48.5</td>
<td>50.0</td>
</tr>
</tbody>
</table>


I-Banking Customers As A Percentage Of Total Customers

The latest wave in IT is internet banking. It is becoming more obvious that the internet has unleashed a revolution that is impacting every sphere of life. With the widespread growth of the internet, customers can use this technology anywhere in the world to access a bank’s network. That’s why customers of I-banking are increasing. It is clear from table 2 that customers of internet banking are also increasing in G-V average rate of increasing customers of I-banking is 33.81 pc which is highest. Other bank groups G-IV, G-I, G-II, G-III have very low rate of increase in customers. It implies I-banking is not very popular among customers due to lack of knowledge.
Table 2
I-Banking Customers As A Percentage of Total Customers

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>G I</td>
<td>0.02</td>
<td>0.05</td>
<td>0.08</td>
<td>0.19</td>
<td>0.58</td>
<td>0.96</td>
<td>2.49</td>
<td>0.62</td>
</tr>
<tr>
<td>G II</td>
<td>.005</td>
<td>0.01</td>
<td>0.01</td>
<td>0.03</td>
<td>0.06</td>
<td>0.17</td>
<td>0.29</td>
<td>0.08</td>
</tr>
<tr>
<td>G III</td>
<td>.005</td>
<td>0.03</td>
<td>0.08</td>
<td>0.13</td>
<td>0.22</td>
<td>0.28</td>
<td>0.55</td>
<td>0.18</td>
</tr>
<tr>
<td>G IV</td>
<td>1.28</td>
<td>1.70</td>
<td>9.37</td>
<td>11.75</td>
<td>19.43</td>
<td>33.30</td>
<td>31.76</td>
<td>15.5</td>
</tr>
<tr>
<td>G V</td>
<td>6.39</td>
<td>7.17</td>
<td>14.08</td>
<td>31.12</td>
<td>43.14</td>
<td>42.24</td>
<td>92.56</td>
<td>33.81</td>
</tr>
</tbody>
</table>

Source: Data Collected Personally From IT Department Of Banks

Impact Of E-Delivery Channels On Bank Groups Profitability

A glance at the table 4 reveals that internet banking has the positive and higher impact on the profitability of all the bank groups except foreign bank group than other e-delivery channels. In case of public sector bank group internet banking has significant effect on profitability. Thus the table concludes that internet banking is very helpful in increasing the profitability of the banks.

Table 4
Impact Of E-Delivery Channels On Bank Groups Profitability

<table>
<thead>
<tr>
<th>Variables</th>
<th>G-I</th>
<th>G-II</th>
<th>G-III</th>
<th>G-IV</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( r )</td>
<td>R</td>
<td>r</td>
<td>R</td>
</tr>
<tr>
<td>NP/Comp.Br.</td>
<td>0.547</td>
<td>0.299</td>
<td>-</td>
<td>0.011</td>
</tr>
<tr>
<td>NP/ATMs</td>
<td>0.512</td>
<td>0.262</td>
<td>-</td>
<td>0.008</td>
</tr>
<tr>
<td>NP/CC</td>
<td>0.284</td>
<td>0.081</td>
<td>0.032</td>
<td>0.001</td>
</tr>
<tr>
<td>NP/IB</td>
<td>0.679*</td>
<td>0.461</td>
<td>0.061</td>
<td>0.004</td>
</tr>
<tr>
<td>NP/MB</td>
<td>0.521</td>
<td>0.271</td>
<td>0.099</td>
<td>0.010</td>
</tr>
<tr>
<td>NP/TB</td>
<td>0.648</td>
<td>0.420</td>
<td>0.049</td>
<td>0.002</td>
</tr>
<tr>
<td>NP/IT</td>
<td>0.582</td>
<td>0.339</td>
<td>-</td>
<td>0.000</td>
</tr>
</tbody>
</table>

Source: Same As Table 1
Internet Banking Risks

Internet banking faces following types of risks

- **Credit Risk**

Credit risk is the risk to earnings or capital arising from an obligator’s failure to meet the terms of any contract with the bank or otherwise to perform as agreed. Internet banking provides the opportunity for banks to expand their geographic range. Customers can reach a given institution from literally anywhere in the world. In dealing with customers over the internet, absent any personal contract, it is challenging for institutions to verify the credentials of their customers which is an important element in making sound credit decision. Verifying collateral and perfecting security agreements also can be challenging with out-of-area borrowers. Unless properly managed, internet banking could lead to a concentration in out-of-area credits.

- **Interest-Rate Risk**

Interest rate risk is the risk to earnings or capital, arising from movements in interest rates. Interest rate risk arises from differences between the timing of rate changes and the timing cash flows. Internet banking can attract deposits, loans and other relationships from a larger pool of possible customers than other forms of marketing. Greater access to customers who primarily seek the best or term reinforces the need for managers to maintain appropriate asset/liability management systems, including the ability to react quickly to changing market conditions.

- **Liquidity Risk**

Liquidity risk is the risk to earnings or capital arising from a bank’s inability to meet its obligations than they come due, without incurring unacceptable losses. Liquidity risk includes the inability to manage unplanned changes in funding sources. Internet banking can increase deposit volatility from customers who maintains accounts solely on the basis of rate or terms. Asset/liability and loan portfolio management system should be appropriate for products offered through internet banking. Increased monitoring of liquidity and changes in deposits and loans may be warranted depending on the volume and nature of internet account activities.

- **Foreign Exchange Risk**

Foreign exchange is present when a loan or portfolio of loans is denominated in a foreign currency or is funded by borrowings in another currency. In some cases, banks will enter into multi-currency credit commitments that permit borrowers to select the currency they prefer to use in each rollover period. Banks may be exposed to foreign exchange risk if they accept deposits from NRIs or create accounts denominated in currencies other than INR on internet banking, although this risk is similar to the real account but internet may provide frequently large
number of transactions. Appropriate system should be developed if banks engage in these activities.

- **Compliance Risk**

Compliance risk is the risk to earnings or capital arising from violations of, or non conformance with laws, rules, regulations, prescribed practices or ethical standards. Compliance risk also arises in situations where the laws or rules governing certain banks products or activities of the bank’s clients may be ambiguous or untested. Most internet banking customers will continue to use other bank delivery channels. Accordingly, banks will need to make certain that their disclosures on internet banking channels, including web sites, remain synchronized with other delivery channels to ensure the delivery of a consistent and accurate message to customers.

- **Strategic Risk**

Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions or lack of strategic goals, the business strategies developed to achieve those goals, the resources deployed these goals and the quality of implementation. The resources need to carry out business strategies are both tangible and intangible. They include communication channels, operating systems, delivery networks and managerial capacities and capabilities. In some cases, banks may offer new products and services via the internet. Sometimes, management does not understand the risk and ramifications of these decisions which cause a loss in the delivery of their product.

- **Reputation Risk**

Reputation risk is the current and prospective impact on earnings and capital arising from negative public opinion. This affects the institution’s ability to establish new relationships or services or continue servicing existing relationships. This risk may expose the institution to litigation, financial loss or a decline in its customer base. Reputation risk exposure is present throughout the organization and includes the responsibility to exercise an abundance of caution in dealing with customer and community. A bank’s reputation can suffer if it fails to deliver on marketing claims or to provide accurate timely services. This can include failing to adequately meet customer credit needs, providing unreliable or inefficient delivery systems, untimely responses to customer inquiries, or violations of customer privacy expectations. Sometimes internet banking services are poorly executed which cause a damage to bank’s reputation.

- **Transaction Risk**

Transaction risk is the current and prospective risk to earnings and capital arising from fraud, errors and inability to deliver products or services, maintain a competitive position and manage information. Transaction risk is evident in each product and service offered and encompasses product development and delivery, transaction processing, system development, computing.
systems, complexity of products and services and the internal control environment. A high level of transaction risk may exist with internet banking products, particularly if these lines of business are not adequately planned, implemented and monitored.

**Strategies To Mitigate The Risk In Internet Banking**

Banks should have sound preventive and detective control to protect their internet banking system from exploitation both internally and externally. They should follow the following measures:

**Access Control**

Logical access control should be implemented on data, systems, application software, utilities, telecommunications lines, libraries, system software etc. Logical access control techniques may include user-ids, passwords or other bio-metric technologies.

**Firewalls**

At the minimum, banks should use the proxy server type of firewalls so that there is no direct connection between the internet and bank’s system. It facilitates a high level of control and in-depth monitoring using logging and auditing tools. For sensitive systems, inspection firewall is recommended which thoroughly inspects all packets of information, and past and present transactions are compared. These generally include a real-time security alert.

**Security Infrastructure**

PKI is the most favored technology for secure internet banking services. However, it is not yet commonly available. While PKI infrastructure is strongly recommended during the transition period, until IDRBT or government puts in place the PKI infrastructure, the following options are recommended:

- Usage of SSL, which ensures server authentication and the use of client side certificates issued by the banks themselves using a certificate server.
- The use of at least 128-bit SSL for securing browser to web server communications and in addition, encryption of sensitive data like passwords in transit within the enterprise itself.

**Penetration Testing**

The information security officer and information system auditor should undertake periodic penetration tests of the system, which could include:

- Attempting to guess passwords using password-cracking tools.
- Search for back door traps in the programs.
- Attempt to overload the system using Ddos (Distributed Denial of Service) & Dos (Denial of Service) attacks.
- Check if commonly known holes in the software, especially the browser and the e-mail...
software exist.

- The penetration testing may also be carried out by engaging outside experts.

**Back Up & Recovery**

The banks should have proper infrastructure and schedules for backing up data. The backed-up data should be periodically tested to ensure recovery without loss of transactions in a time frame as given out in the bank’s security policy. Business continuity should be ensured by having disaster recovery also be tested periodically.

**Maintenance Of Infrastructure**

Security infrastructure should be properly tested before using the systems and applications for normal operations. The bank should upgrade the systems by installing patches released by the developers to remove bugs and loopholes and upgrade to newer versions which give better security and control.

**Other Measures**

- It is important for banks to be familiar with the regulations that permit electronic delivery of disclosures/notices versus those that require traditional hard copy notification. Banks should carefully review and monitor all requirements applicable to electronic products and services and ensure they comply with evolving statutory and regulatory requirements.

- Before introducing a internet product, management should consider whether the product and technology are consistent with tangible business objectives in the bank’s strategic plan. The bank should consider whether adequate expertise and resources are available to identify, monitor, control risk in the internet banking business. The planning and decision making process should focus on how a specific business need is met by the internet banking product, rather than focusing on the product as an independent objective.

- Banks should carefully consider how connections to third party are presented on their web sites. Hypertext links are often used to enable a customer to link to a third party. Such link may reflect an endorsement of the third party’s products or services in the eyes of the customer. It should be clear to the customer when they left the bank’s web site so that there is no confusion about the provider of the specific products and services offered or the security and privacy standards that apply.

**Implication**

The present study shows high impact of bank group profitability. It is the time to mitigate the various types of risk particularly of internet because internet is extensively used in the various banks. This mitigation will create the trust and confidence of the internet customers.
Conclusion

Thus the study concludes that internet banking has created many types of risk but these risks can be easily mitigated. It is also a need of time to mitigate the risk to make the technology effective because without technology banks cannot become efficient and productive.

References