Risk Management of Internet Banking

Shapoor Zarei
Professor of Information Technology; Dey Bank of Iran
Teharan, Iran
info@zarei.me

Abstract
Cost effective delivery channel of E-banking services, technological innovations and competition among existing banking organizations are the major driving forces behind the rapid spread of E-banking all over the world. However, the rapid development of E-banking carries risks as well as benefits. Hence the banks must be conscious of different types of risks to remain efficient and cost effective. The E-banking sectors in Iran have been also developed in recent years. Nowadays, Iranian banks compete to get a better position in the banking system. Hence they should apply risk management strategies not only to get the better position but also to increase customer acceptance.
Therefore in this paper a generic set of risks are discussed as the basis for formulating general risk control guidelines. These risks are classified into eight categories involving security risks, legal and ethical risks, reputational risks, operational risks, money laundering risk, strategic risks, cross border risks and traditional risks.

Keywords: Internet banking, E-Banking, Risk Management, strategic Risk

1.Introduction

Banks have been using electronic and telecommunication networks for delivering a wide range of value added products and services over a long time. The delivery channels include direct dial – up connections, private networks, public networks etc. and the devices include telephone, Personal Computers, Automated Teller Machines etc. With the popularity of PCs, easy access to Internet and World Wide Web (WWW), Internet is increasingly used by banks as a channel for receiving instructions and delivering their products and services to their customers [6]. This form of banking is generally referred to as Internet Banking. Banking on the Internet provides benefits to the consumer in terms of convenience, and to the provider in terms of cost reduction and greater reach. Along with reduction in cost of transactions, it has also brought about a new orientation to risks and even new forms of risks to which banks conducting internet banking expose themselves. While banks should remain efficient and cost effective, they must be conscious of different types of risks that the internet as a media entails and also have systems in place to manage these risks. Because of rapid changes in information technology, there is no finality either in the types of risks or their control measures and risk management strategies.

The E-banking sectors in Iran have been also developed in recent years. Nowadays, Iranian banks compete to get a better position in the banking system. Hence they should apply risk management strategies not only to get the better position but also to increase customer acceptance. Therefore the main purpose of this paper is to identify a generic set of risks as the basis for formulating general risk control guidelines. These risks are classified into eight categories involving security risks, legal and ethical risks, reputational risks, operational risks, money laundering risk, strategic risks, cross border risks and traditional risks.

ISBN: 978-960-474-273-8

2. Internet Banking Risks

Banking on the Internet provides benefits to the consumer in terms of convenience, and to the provider in terms of cost reduction and greater reach. The Internet itself however is not a secure medium, and thus poses a number of risks of concern to regulators and supervisors of banks and financial institutions. As figure 1 shows the risks associated with internet banking are categorized into eight categories.

Figure 1. Risks Associate with Internet Banking

2.1 Security Risks

Internet is a public network of computers which facilitates flow of data / information and to which there is unrestricted access. Therefore banks using this medium for financial transactions must have proper technology and systems in place to build a secured environment for such transactions. Security risk arises on account of unauthorized access to a bank's critical information stores like accounting system, risk management system, portfolio management system, etc. A breach of security could result in direct financial loss to the bank. For example, hackers operating via the internet could access, retrieve and use confidential customer information and also can implant virus. This may result in loss of data, theft of or tampering with customer information, disabling of a significant portion of bank's internal computer system thus denying service, cost of repairing these etc. Other related risks are loss of reputation, infringing customers' privacy and its legal implications etc.

Thus, access control is of paramount importance [2]. Controlling access to banks' system has become more complex in the Internet environment which is a public domain and attempts at unauthorized access could emanate from any source and from anywhere in the world with or without criminal intent. Attackers could be hackers, unscrupulous vendors, disgruntled employees or even pure thrill seekers. Also, in a networked environment the security is limited to its weakest link. It is therefore, necessary that banks critically assess all interrelated systems and have access control measures in place in each of them.

In addition to external attacks banks are exposed to security risk from internal sources e.g. employee fraud. Employees being familiar with different systems and their weaknesses become potential security threats in a loosely controlled environment. They can manage to acquire the authentication data in order to access the customer accounts causing losses to the bank. Unless specifically protected, all data / information transfer over the Internet can be monitored or read by unauthorized persons. There are programs such as 'sniffers' which can be set up at web servers or other critical locations to collect data like account numbers, passwords, account and credit card numbers. Data privacy and confidentiality issues are relevant even when data is not being transferred over the net. Data residing in web servers or even banks' internal systems are susceptible to corruption if not properly isolated through firewalls from Internet.

The risk of data alteration, intentionally or unintentionally, but unauthorized is real in a networked environment, both when data is being transmitted or stored. Proper access control and technological tools to ensure data integrity is of utmost importance to banks. Another important aspect is whether the systems are in place to quickly detect any such alteration and set the alert.

Identity of the person making a request for a service or a transaction as a customer is crucial to legal validity of a transaction and is a source of risk to a bank. A computer connected to Internet is identified by its IP (Internet Protocol) address. There are

ISBN: 978-960-474-273-8

methods available to masquerade one computer as another, commonly known as 'IP Spoofing'. Likewise user identity can be misrepresented. Hence, authentication control is an essential security step in any e-banking system.

Non-repudiation involves creating a proof of communication between two parties; say the bank and its customer, which neither can deny later. Banks' system must be technologically equipped to handle these aspects which are potential sources of risk.

2.2 Legal and ethical Risks

Legal risk arises from violation of, or non-conformance with laws, rules, regulations, or prescribed practices, or when the legal rights and obligations of parties to a transaction are not well established. Given the relatively new nature of Internet banking, rights and obligations in some cases are uncertain and applicability of laws and rules is uncertain or ambiguous, thus causing legal risk. Other reasons for legal risks are uncertainty about the validity of some agreements formed via electronic media and law regarding customer disclosures and privacy protection. A customer inadequately informed about his rights and obligations, may not take proper precautions in using Internet banking products or services, leading to disputed transactions, unwanted suits against the bank or other regulatory sanctions.

In the enthusiasm of enhancing customer service, bank may link their Internet site to other sites also. This may cause legal risk. Further, a hacker may use the linked site to defraud a bank customer. If banks are allowed to play a role in authentication of systems such as acting as a Certification Authority, it will bring additional risks. A digital certificate is intended to ensure that a given signature is, in fact, generated by a given signer [1]. Because of this, the certifying bank may become liable for the financial losses incurred by the party relying on the digital certificate.

2.3 Reputational Risks

Reputational risk is the risk of getting significant negative public opinion, which may result in a critical loss of funding or customers. Such risks arise from actions which cause major loss of the public confidence in the banks' ability to perform critical functions or impair bank-customer relationship. It may be due to banks' own action or due to third party action. The main reasons for this risk may be system or product not working to the expectations of the customers, significant system deficiencies, significant security breach both due to internal and external attack, inadequate information to customers about product use and problem resolution procedures, significant problems with communication networks that impair customers' access to their funds or account information especially if there are no alternative means of account access. Such situation may cause customer-discontinuing use of product or the service. Directly affected customers may leave the bank and others may follow if the problem is publicized.

2.4 Operational Risks

Operational risk, also referred to as transactional risk is the most common form of risk associated with internet banking [4]. It takes the form of inaccurate processing of transactions, non enforceability of contracts, compromises in data integrity, data privacy and confidentiality, unauthorized access / intrusion to bank's systems and transactions etc. Such risks can arise out of weaknesses in design, implementation and monitoring of banks' information system. Besides inadequacies in technology, human factors like negligence by customers and employees, fraudulent activity of employees and crackers / hackers etc. can become potential source of operational risk. Often there is thin line of difference between operational risk and security risk and both terminologies are used interchangeably.

2.5. Money Laundering Risk

As Internet banking transactions are conducted remotely, banks may find it difficult to apply traditional method for detecting and preventing undesirable criminal activities. Application of money laundering rules may also be inappropriate for some forms of electronic payments. Thus banks expose themselves to the money laundering risk. This may result in legal

sanctions for non-compliance with "know your customer" laws. To avoid this, banks need to design proper customer identification and screening techniques, develop audit trails, conduct periodic compliance reviews, frame policies and procedures to spot and report suspicious activities in Internet transactions.

2.6. Strategic Risks

This risk is associated with the introduction of a new product or service. Degree of this risk depends upon how well the institution has addressed the various issues related to development of a business plan, availability of sufficient resources to support this plan, credibility of the vendor if outsourced and level of the technology used in comparison to the available technology etc. For reducing such risk, banks need to conduct proper survey, consult experts from various fields, establish achievable goals and monitor performance. Also they need to analyze the availability and cost of additional resources, provision of adequate supporting staff, proper training of staff and adequate insurance coverage. Due diligence needs to be observed in selection of vendors, audit of their performance and establishing alternative arrangements for possible inability of a vendor to fulfill its obligation . Besides this, periodic evaluations of new technologies and appropriate consideration for the costs of technological up-gradation are required [3].

2.7 Cross border risks

Internet banking is based on technology that, by its very nature, is designed to extend the geographic reach of banks and customers. Such market expansion can extend beyond national borders. This causes various risks. It includes legal and regulatory risks, as there may be uncertainty about legal requirements in some countries and jurisdiction ambiguities with respect to the responsibilities of different national authorities. Such considerations may expose banks to legal risks associated with non-compliance of different national laws and regulations, including consumer protection laws, record-keeping and reporting requirements, privacy rules and money laundering laws.

If a bank uses a service provider located in another country, it will be more difficult to monitor it thus, causing operational risk. Also, the foreign-based service provider or foreign participants in Internet banking are sources of country risk to the extent that foreign parties become unable to fulfill their obligations due to economic, social or political factors. Cross border transaction accentuates credit risk, since it is difficult to appraise an application for a loan from a customer in another country compared to a customer from a familiar customer base.

Banks accepting foreign currencies in payment for electronic money may be subjected to market risk because of movements in foreign exchange rates.

2.8 Traditional risks

Traditional banking risks such as credit risk, liquidity risk, interest rate risk and market risk are also present in Internet banking. These risks get intensified due to the very nature of Internet banking on account of use

ISBN: 978-960-474-273-8

of electronic channels as well as absence of geographical limits [5]. However, their practical consequences may be of a different magnitude for banks and supervisors than operational, reputational and legal risks. This may be particularly true for banks that engage in a variety of banking activities, as compared to banks or bank subsidiaries that specialize in Internet banking.

Credit risk is the risk that a counter party will not settle an obligation for full value, either when due or at any time thereafter. Banks may not be able to properly evaluate the credit worthiness of the customer while extending credit through remote banking procedures, which could enhance the credit risk. Presently, banks generally deal with more familiar customer base. Facility of electronic bill payment in Internet banking [1] may cause credit risk if a third party intermediary fails to carry out its obligations with respect to payment. Proper evaluation of the creditworthiness of a customer and audit of lending process are a must to avoid such risk.

Another facility of Internet banking is electronic money It brings various types of risks associated with it. If a bank purchases e-money from an issuer in order to resell it to a customer, it exposes itself to credit risk in the event of the issuer defaulting on its obligation to redeem electronic money.

Liquidity Risk arises out of a bank's inability to meet its obligations when they become due without incurring unacceptable losses, even though the bank may ultimately be able to meet its obligations. It is important for a bank engaged in electronic money transfer activities that it ensures that funds are adequate to cover redemption and settlement demands at any particular time. Failure to do so, besides exposing the bank to liquidity risk, may even give rise to legal action and reputational risk.

Similarly banks dealing in electronic money face interest rate risk because of adverse movements in interest rates causing decrease in the value of assets relative to outstanding electronic money liabilities. Banks also face market risk because of losses in on-and-off balance sheet positions arising out of movements in market prices including foreign exchange rates. Banks accepting foreign currency in payment for electronic money are subject to this type of risk.

Internet banking is going to intensify the competition among various banks. The open nature of Internet may induce a few banks to use unfair practices to take advantage over rivals. Any leaks at network connection or operating system etc., may allow them to interfere in a rival bank's system.

3. Conclusion

Along with the benefits, Internet banking carries various risks for bank itself as well as banking system as a whole. The rapid pace of technological innovation is likely to keep changing the nature and scope of risks banks face. These risks must be balanced against the benefits. Supervisory and regulatory authorities are required to develop methods for identifying new risks, assessing risks, managing risks and controlling risk exposure. But authorities need to keep in consideration that the development and use of Internet banking are still in their early stages, and policies that hamper useful innovation and experimentation should be avoided. Thus authorities need to encourage banks to develop a risk management process rigorous and comprehensive enough to deal with known risks and flexible enough to accommodate changes in the type and intensity of the risks.

References

[1] Doroodchi, M., Nikmehr, N., & Iran mehr, A. (2007). Survey on electronic payment systems in ecommerce. *1st international E-banking conference* . Tehran.

[2] Doroodchi, M., Nikmehr, N. (2008). Survey On E-Payment Systems through analytic Hierarchy Process: Retail Stores in Iran. *1st International E-city Conference*. Tehran.

[3] Edelman, A. , Longcope, D. , Miller, J., Obbink, K., Oudshoom, J. & Wolff, R. (2007). "MSU Information Technology Strategic Plan". *Montana State University*.

[4] FFIEC Information Technology Examination Handbook, "Management booklet, Risk Overview". [online]. < http://www.ffiec.gov/ffiecinfobase/booklets/mang/02.html > [July 2008]

[5] Jayawardhena, C., & Foley, P. (2000). Changes in the banking sector – the case of Internet banking in the UK. *Internet Research* , 19-31.

[6] Kannan, R., Project on Internet Banking, "Report of RBI Working Group Formation of The Working Group & its Terms of Reference". [online], <htttp://www.geocities.com/kstability/student/internet-banking/index.html> [June 2008]