Electronic Banking Groom And Risks Identification

Dr. Rakesh Kumar Ray

Assistant Professor Department of Forensic Science School of Life Sciences,

Swami Vivekanand University,Sagar(M.P)

ABSTRACT

Electronic payment media are likely to figure importantly in the development of electronic commerce, and retail electronic banking services and products, including electronic money, could provide significant new opportunities for banks. Electronic banking may allow banks to expand their markets for traditional deposit-taking and credit extension activities, and to offer new products and services or strengthen their competitive position in offering existing payment services. In addition, electronic banking could reduce operating costs for banks.

INTRODUCTION

Electronic banking groom with speed that no one expected, industry growth is awesome in a little span of time. E-Banking offer number of services and products that was unpredictable during the manual banking era banks has limited boundaries and the source of competitive advantage is very difficult to obtain. Man power was the only weapon to get advantage over the benefits.

E-Banking benefits can't be denied but on the other hand the risks are on high side. The banks require keeping the balance of benefits versus risk. The marketed offerings welcome the huge customer base but to retain the customer lot of homework need to be done by the banks.

The risks related to E-banking are categories to define it more specifically in order to develop risk mitigation strategy. The reach of the customer is both nationally and internally and banks have to face beyond the national boundaries to resolve their customer problem. The open and close network of E-banking increases the complexity; close ended channels include all the delivery channels offered by the bank on the other hand open ended networks like internet is subjected to security and reputational risk.

The risks related with E-banking are needed to identified, manage and control. The rules and regulation should be define by the central authority and share it with all the banking organization in order to reduce the level of risk. The risk can be measure on both quantities and qualitative way.

The risk management can't be same for every bank, and it's very difficult to apply same rule to every banking organization because change in technology is unpredictable, size and the infrastructure of the bank matters. This report will discuss the risk management strategy based on some basic characteristics of E-Banking.

In many ways, e-banking is not unlike traditional payment, inquiry, and information processing systems, differing only in that it utilizes a different delivery channel. Any decision to adopt e-banking is normally influenced by a number of factors. These include customer service enhancement and competitive costs, all of which motivate banks to assess their electronic commerce strategies. The benefits of e-banking are widely known and will only be summarized briefly in this document.

E-banking can improve a bank's efficiency and competitiveness, so that existing and potential customers can benefit from a greater degree of convenience in effecting transactions. This increased level of convenience offered by the bank, when combined with new services, can expand the bank's target customers beyond those in traditional markets. Consequently, financial institutions are therefore becoming more aggressive in adopting electronic banking capabilities that include sophisticated marketing systems,

Remote-banking capabilities, and stored value programs. Internationally, familiar examples include telephone banking, automated teller networks, and automated clearinghouse systems. Such technological advances have brought greater sophistication to all users, commercial and "the man in the street".

A bank may be faced with different levels of risks and expectations arising from electronic banking as opposed to traditional banking. Furthermore, customers who rely on e-banking services may have greater intolerance for a system that is unreliable or one that does not provide accurate and current information. Clearly, the longevity of E-banking depends on its accuracy, reliability and accountability. The challenge for many banks is to ensure that savings from the electronic banking technology more than offset the costs.

Scope:

This report discusses the types of risk associated with E-banking, methods to assess the risk and finally management of risk with respect to BCP /DR .

In 1950, the Bank of America (then the largest bank in the world) asked SRI to assess the possibility of developing electronic computers that could take over the labor-intensive banking tasks of handling checks and balancing accounts. The creation of branch offices and the rapidly increasing number of checks being used by a growing clientele threatened to overwhelm the existing manual processing and record keeping. At that time, no large-scale electronic machine for any bank was under development existing computers were used mostly for scientific calculations. They were unreliable, and had extremely limited input and output capability. In spite of this, SRI's feasibility study, issued in May 1951, was sufficiently encouraging for the Bank of America to authorize a major multi-year development effort.

We now take for granted the many ways that computers assist individuals and businesses. The 50-plus-year-old project briefly described here provided a vision of what business could expect from the application of data-processing machines, and illustrates how and why some of the key capabilities were invented, including bookkeeping, optical character recognition (OCR or scanning), and robotic document sorting. The automated teller machine (ATM) is the natural descendant of this work, and illustrates the progression away from paper checks toward all electronic banking.

E-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, 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. While the risks and controls are similar for the various e-banking access channels, this report focuses specifically on Internet-based services due to the Internet's widely accessible public network. Accordingly, this report begins with a discussion of the two primary types of Internet websites: informational and transactional.

Impact of e-banking on traditional services:

Before talking about the issues of risks and responses to E banking, we would like to spend a little time considering the wider question of what the e-banking revolution might mean for the future. we take "E" to mean anything electronic whether it be Internet, television, telephone or all three.

One of the issues currently being addressed is the impact of e-banking on traditional banking players. After all, if there are risks inherent in going into e-banking there are other risks in not doing so. It is too early to have a firm view on this yet. Even to practitioners the future of e-banking and its implications are unclear. It might be convenient nevertheless to outline briefly two views that are prevalent in the market.

The view that the Internet is a revolution that will sweep away the old order holds much sway. Arguments in favor are as follows:

E-banking transactions are much cheaper than branch or even phone transactions. This could turn yesterday's competitive advantage – a large branch network – into a comparative disadvantage, allowing e-banks to undercut bricks-and-mortar banks. This is commonly known as the "beached dinosaur" theory.

E-banks are easy to set up so lots of new entrants will arrive. 'Old-world' systems, cultures and structures will not encumber these new entrants. Instead, they will be adaptable and responsive. E-banking gives consumers much more choice. Consumers will be less inclined to remain loyal.

E-banking will lead to an erosion of the 'endowment effect' currently enjoyed by the major UK banks. Deposits will go elsewhere with the consequence that these banks will have to fight to regain and retain their customer base. This will increase their cost of funds, possibly making their business less viable. Lost revenue may even result in these banks taking more risks to breach the gap.

Portal providers are likely to attract the most significant share of banking profits. Indeed banks could become glorified marriage brokers. They would simply bring two parties together e.g. buyer and seller, payer and payee.

The products will be provided by monoclines, experts in their field. Traditional banks may simply be left with payment and settlement business even this could be cast into doubt.

Traditional banks will find it difficult to evolve. Not only will they be unable to make acquisitions for cash as opposed to being able to offer shares, they will be unable to obtain additional capital from the stock market. This is in contrast to the situation for Internet firms for whom it seems relatively easy to attract investment.

There is of course another view which sees e-banking more as an evolution than a revolution.

E-banking is just banking offered via a new delivery channel. It simply gives consumers another service (just as ATMs did).

Like ATMs, e-banking will impact on the nature of branches but will not remove their value.

Experience in Scandinavia (arguably the most advanced e-banking area in the world) appears to confirm that the future is 'clicks and mortar' banking. Customers want full service banking via a number of delivery channels. The future is therefore 'Martini Banking' (any time, any place, anywhere, anyhow).

Electronic banking Delivery Channels:

E-Banking transaction needs some interface to communicate with banking customer. All the electronic transaction performs through some interfaces. The electronic devices which perform interact with customers and communicate with other banking system is called electronic banking delivery channels.

Following are the electronic banking delivery channels.

ATM:

An automated teller machine (ATM) is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions in a public space without the need for a human clerk or bank teller. On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smartcard with a chip, that contains a unique card number and some security information, such as an expiration date or CVC (CVV). Security is provided by the customer entering a personal identification number (PIN).
Using an ATM, customers can access their bank accounts in order to make cash withdrawals (or credit card cash advances) and check their account balances as well as purchasing mobile cell phone prepaid credit. ATMs are known by various other names including automated banking machine, money machine, bank machine, cash machine, hole-in-the-wall, cash point.
IVR (Interactive Voice Response):

voice exchange is the E-Banking delivery channel used for transaction using telecom infrastructure. User dials the number and selects the option using key punch, operator response on every key press. Customer gives his identification by providing his NIC and TPIN.

CDM (Cash Deposit Machine):

Cash deposit machine is the electronic machine used to deposit the cash, check. CDM scan the cash or check and deposit the amount in his or her
Provided account number.

POS (Point of Sale):

Point of sale used for retail transaction device, customer perform transaction by swapping the card on POS machine. Most of the customer used debit or credit card for purchasing transaction. Different payment gateway offers their services to banks such as VISA, Master etc.

Risk:

A state of uncertainty where some of the possibilities involve a loss, catastrophe, or other undesirable outcome.

Types of E-Banking Risks:

The risks associated with E-Banking are the following.

· Strategic Risk

· Business Risk

· Operational Risk

· Security Risk

· Reputational Risk

· Legal Risk

Strategic Risk:

On strategic risk E-banking is relatively new and, as a result, there can be a lack of understanding among senior management about its potential and implications. People with technological, but not banking, skills can end up driving the initiatives. E-initiatives can spring up in an incoherent and piecemeal manner in firms. They can be expensive and can fail to recoup their cost. Furthermore, they are often positioned as loss leaders (to capture market share), but may not attract the types of customers that banks want or expect and may have unexpected implications on existing business lines.

Business risks:

Business risks are also significant. Given the newness of e-banking, nobody knows much about whether e-banking customers will have different characteristics from the traditional banking customers. They may well have different characteristics – e.g. I want it all and I want it now. This could render existing score card models inappropriate, thus resulting in either higher rejection rates or inappropriate pricing to cover the risk. Banks may not be able to assess credit quality at a distance as effectively as they do in face to face circumstances. It could be more difficult to assess the nature and quality of collateral offered at a distance, especially if it is located in an area the bank is unfamiliar with (particularly if this is overseas). Furthermore as it is difficult to predict customer volumes and the stickiness of e-deposits (things which could lead either to rapid flows in or out of the bank) it could be very difficult to manage liquidity. Of course, these are old risks with which banks and supervisors have considerable experience but they need to be watchful of old risks in new guises. In particular risk models and even processes designed for traditional banking may not be appropriate.

Banks face three main types of operations risk:
· volume forecasts
· Management information systems and
· Outsourcing.

Accurate volume forecasts have proved difficult – One of the key challenges encountered by banks in the Internet environment is how to predict and manage the volume of customers that they will obtain. Many banks going on-line have significantly misjudged volumes. When a bank has inadequate systems to cope with demand it may suffer reputational and financial damage, and even compromises in security if extra systems that are inadequately configured or tested are brought on-line to deal with the capacity problems.

As a way of addressing this risk, banks should:
· undertake market research,
· adopt systems with adequate capacity and scalability,
· undertake proportionate advertising campaigns, and
· Ensure that they have adequate staff coverage and develop a suitable business continuity plan.

In brief, this is a new area, nobody knows all the answers, and banks need to exercise particular caution.

The second type of operations risk concerns management information systems. Again this is not unique to E-banking. I have seen many banks venture into new areas without having addressed management information issues. Banks may have difficulties in obtaining adequate management information to monitor their e-service, as it can be difficult to establish/configure new systems to ensure that sufficient, meaningful and clear information is generated. Such information is particularly important in a new field like e-banking. Banks are being encouraged by the FSA to ensure that management have all

the information that they require in a format that they understand and that does not cloud the key information with superfluous details.

Finally, a significant number of banks offering e-banking services outsource related business functions, e.g. security, either for reasons of cost reduction or, as is often the case in this field, because they do not have the relevant expertise in-house. Outsourcing a significant function can create material risks by potentially reducing a bank's control over that function.

Security Risk:

Security issues are a major source of concern for everyone both inside and outside the banking industry. E-banking increases security risks, potentially exposing hitherto isolated systems to open and risky environments. Both the FSA and banks need to be proactive in monitoring and managing the security threat.

Security breaches essentially fall into three categories; breaches with serious criminal intent (e.g. fraud, theft of commercially sensitive or financial information), breaches by 'casual hackers' (e.g. defacement of web sites or 'denial of service' – causing web sites to crash), and flaws in systems design and/or set up leading to security breaches (e.g. genuine users seeing / being able to transact on other users' accounts). All of these threats have potentially serious financial, legal and reputational implications.

Many banks are finding that their systems are being probed for weaknesses hundreds of times a day but damage/losses arising from security breaches have so far tended to be minor. However some banks could develop more sensitive "burglar alarms", so that they are better aware of the nature and frequency of unsuccessful attempts to break into their system.

The most sensitive computer systems, such as those used for high value payments or those storing highly confidential information, tend to be the most comprehensively secured. One could therefore imply that the greater the potential loss to a bank the less likely it is to occur, and in general this is the case. However, while banks tend to have reasonable perimeter security, there is sometimes insufficient segregation between internal systems and poor internal security. It may be that someone could breach the lighter security around a low value system, e.g. a bank's retail web site, and gain entry to a high value system via the bank's internal network. We are encouraging banks to look at the firewalls between their different systems to ensure adequate damage limitation should an external breach occur. As ever though, the greatest threat so far has been from the enemy within – i.e. your own employees, contractors and so on.

It is easy to overemphasize the security risks in e-banking. It must be remembered that the Internet could remove some errors introduced by manual processing (by increasing the degree of straight through processing from the customer through banks' systems). This reduces risks to the integrity of transaction data (although the risk of customers incorrectly inputting data remains). As e-banking advances, focusing general attention on security risks, there could be large security gains.

Reputational Risks:

Finally, with regard to risks, I would mention reputational risk. This is considerably heightened for banks using the Internet. For example the Internet allows for the rapid dissemination of information which means that any incident, either good or bad, is common knowledge within a short space of time. Internet rumors can easily become self-fulfilling prophecies. The speed of the Internet considerably cuts the optimal response times for both banks and regulators to any incident. Banks must ensure their crisis management, particularly PR, processes are able to cope with Internet related incidents (whether they be real or hoaxes).

Any problems encountered by one firm in this new environment may affect the business of another, as it may affect confidence in the Internet as a whole. There is therefore a risk that one rogue e-bank could cause significant problems for all banks providing services via the Internet. This is a new type of systemic risk and is causing concern to e-banking providers. Overall, the Internet puts an emphasis on reputation risks. Never before has the bank's shop window (ie its site) been so important.

One last reputational risk will be familiar to us all. That is whether the products being sold over the net are being marketed in such a way that the bank will be protected against future charges of mis-selling. As in the physical, so in the virtual world. Banks need to be sure those customers' rights and information needs are adequately safeguarded and provided for.

Legal Risk:

The bank not following the rules and regulation for E-banking, normally risk mainly arise from virtual bank when E-banking services are offered without complying the rule and regulation of other countries.

Risk Assessment:

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

Risk is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization.
To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data). The risk assessment methodology encompasses nine primary steps, which are briefly defined in following part.

System Characterization:

In assessing risks for an IT system, the first step is to define the scope of the effort. Generally we categorize it in to two main components i.e. IT systems and operating environment. In IT system we usually look into hardware, software, system connectivity, and responsible division or support personnel whereas in operating environment we look in to functional and technical requirements, security policies, and level of protection towards data and network topologies.

Threat Identification:

The goal of this step is to identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the IT system being evaluated. Due to these threats potential vulnerabilities that system contains has also been delineated so that possible remedies for existing controls must be taken into account.

Vulnerability Identification:

The target for this identification is to develop a checklist for all the vulnerabilities that may exploit different threat sources. Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.

Control Analysis:

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.

Likelihood Determination:

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment.

Impact Analysis;

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information:

• System mission (e.g., the processes performed by the IT system)

• System and data criticality (e.g., the system's value or importance to an organization)

• System and data sensitivity.

Risk Determination:

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of:

• The likelihood of a given threat-source's attempting to exercise a given vulnerability
• The magnitude of the impact should a threat-source successfully exercise the vulnerability
• The adequacy of planned or existing security controls for reducing or eliminating risk.

Control Recommendations:

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level.

Risk Mitigation and Control:

Control recommendations:

Our recommendations for all this assessment are following:

- Effectiveness of recommended options
- Legislation and regulations
- Organizational policy
- Safety and reliability

Effectiveness of recommended options:

It is the responsibility of the IT security specialist to know about the known threats prior to attack and must follow the policy that dictates continuity of the business in adverse conditions.

Legislation and regulations:

To facilitate nation wide E banking India has now drafted E-banking law which gives coverage to all types of electronic frauds. Besides that State bank of India has also circulated necessary action taken in case of disaster.

Organizational policy:

Since SBP enforce policy for all banks to have there DR site available in all times when the continuity of the business has been scarified. Therefore organizational policy for the bank is to maintain complete backup of there data on daily basis and on real time in case of backing up the financials transactions. In this context bank is using to types of communication channel with DR sites. First one is through land line networks a service by Cyber net and also radio link as secondary backup channel.

Safety and reliability:

In general, network intrusion detection has been done through various intrusion detection systems. Proper disposal of ex-employee identity from the systems has been done. Two factor authentications shall be done on data center or through biometrics at least. Proper authorizations have been given to people who access sensitive data. Proper backups shall be taken to avoid any unnecessary data loss.

Conclusion:

Modern electronic banking concept in the banking services is new for people. Most of our bank has not any marketing or sales forces to execute the raw and cold business of electronic banking for their own organization. People are not also conscious about the advantages of the technology. Some multinational banks are already introduced their marketing activities over their targeted customers for specialized products like electronic products which is found very effective. The multinationals are coming up towards people with variety of highly technical products, which can solve people's problem and can able to modernize their lifestyle. The growth of electronic banking users increasing is a significant manner. However, last 10 years it has got tremendous importance over the bank customer and hopefully it will increase day by day after nurture the product by the professional bankers.

References:

[1] Risk management Guide for Information technology Gray Stonebunner, Alice Goguen, and Alexis feringa

[2] Business Countitinuty and Distaster Recovery Susan Snedaker

[3] Risk Management Principles of Electronic Banking ww.bis.org/publ/bcbs98.pdf

[4] Internet banking in Indian

[5] Manjusha Goel- Impact of Technology on Banking Sector –Internal Journal of Scientific research, in India, Volume : 2 | Issue : 5 | May 2013 • ISSN No 2277 – 8179.

[6] w.w.w.google.com