Risk Assessment of Technology Change in Financial Sector

Lim Qian Pink and Mohd Ridzuan Darun

A review of current risk management practices among Internet banking providers is presented given the increasing breach of security incidents worldwide. In-depth analysis is performed using Internet banking guidelines issued by three central banks (Central Bank of Malaysia, Monetary Authority of Singapore and Hong Kong Monetary Authority). Three distinctive risks are identified (informational security, transactional and strategic risks) as the most relevant among the guidelines studied. These risks are then mapped against threats towards achieving bank’s goals using Sheehan’s Risk Based Approach to Strategy Execution framework. The likelihood and magnitude of each risk was evaluated based on different perspectives proposed in the strategy map. The analysis concludes that gradual migration towards internalisation of essential processes is central to improving internet banking security. Future research should aim to gather richer sources of information through interviews with banking personnel to gain better insight into risks and how they are managed.

Track: Contemporary Issues in Finance, Risk Management Process

1. Introduction

The adoption of technology into the financial sector has benefited the financial sector greatly. The role of a bank’s physical branch as market penetration tool is being gradually taken over by Internet banking which offers faster, reliable and hassle-free services. This is evidenced by DeYoung et al (2007) research where there is high positive correlation between Internet adoption and profits of US community banks. Similarly, Claeys and Arnaboldi (2008) discovered that European banks that offered internet banking possessed higher competitive edge than their branch counterparts.

2. Literature Review

2.1. Supremacy of Internet Banking

Banking institutions globally have digitalised their operation and offered Internet banking facilities as additional banking products since 1990s. Malaysia has joined the bandwagon after Central Bank of Malaysia (BNM) gave the green light to domestic banks to offer Internet banking service in 2000 and subsequently foreign banks to do the same in 2002 (Radhakrishna, 2009). As a result, Internet banking in Malaysia has the highest percentage of turnover to GDP of 188.5% in comparison of other payment channels (Bank Negara Malaysia, 2012). In countries like USA, Europe and Hong Kong, there are banks which go so far as to adopt an Internet-only business approach. While there are undeniable benefits to internet banking, there are also insidious threats lurking at every corner. It is therefore imperative that proper risk management be conducted to reduce these risks to acceptable levels.
2.2. Threats to Internet Banking

The use of the internet enables unlimited access into banks’ internal system by unknown third party and this is beyond banks’ peripheral control. This accentuates existing risk faced by banks, leaving them vulnerable to external attacks. An estimation of USD8.9 million was spent annually to recover from cyber attack in the US, Germany and Japan in 2011 (Messer, 2012). Passeri (2013) reported a worrisome trend of increasing cyber attacks with 50 percent occurrence on a monthly average. These malicious attacks will result not only in financial losses but also loss of customer confidence in the banking system.

The loss of trust in Internet service will affect banks’ reputation severely and lead to financial instability. The recent series of cyber attacks in the USA have put many Internet banking services providers under public scrutiny. Distributed Denial of Service (DDOS) attacks by hackers have crippled banking operations of banks such Bank of America, JP Morgan and Wells Fargo for hours and days, affecting millions of customers (Menn, 2013). These attacks have prompted various quarters to revisit the effectiveness of their risk management policies in managing technology related risks.

3. Methodology

Sheehan (2010) risk based approach to strategy execution framework has been adopted to assess risks associated to Internet banking. Since any threat to a bank’s goals is viewed as a risk, this framework aims to isolate risks by working backwards from the goals. First, a strategy map for the business is created. The risks are then identified based on the strategy map and the magnitude and likelihood of each risk is assessed. Finally, the risk management methods are incorporated into the strategy map bringing the process full circle.

3.1. Strategy Map

The strategy map in Figure 1 illustrates what Internet banking providers aim to achieve and the means to these goals. The four perspectives are fundamental components of any business and aim to summarize the strategy used to achieve the business’ vision and mission. The financial perspective simply reiterates the bank’s vision by seeking to lower costs while increasing revenue and productivity. This is achieved through operational excellence – by providing customers with speedy, reliable, secure and generally consumer centric services.

The act of satisfying customers in turn requires closer examination of the inner workings of the internet banking business. These can be categorized into the customer, operational, innovation and regulatory and social processes. The customer process activities involve marketing and branding initiatives for business products and services. Operational processes of Internet banking involve information requests, order processing, business transactions and information dissemination. Since the internet banking business is driven by technology change, innovation of products and service offerings is vital for banks to stay ahead of the competition.
The innovation process covers any activity which improves the business from the financial perspective including offering new and differentiated services, improving efficiency of IT systems and enforcing better monitoring and countermeasures against cyber-attacks. Lastly, Internet banking providers need to make sure they comply with the regulatory requirements by their respective financial regulators in conducting the business.

The learning and growth perspective illustrates the resources needed to perform processes smoothly and effectively. Running Internet banking business requires support from high level management and skilled personnel who are well versed in technology development. On top of that, banks need to manage their information capital such as having the latest IT systems that can cope with changes of technology and fend off security threats.
3.2. Risk Identification

Risks are internal and external events that have negative impact on the business’ financial performance. These risks can be identified from the perspectives in the strategy map. The process involves identifying actions or the lack thereof that result in outcomes which are unfavorable to each component of the strategy map. For example, when identifying risks from the customer perspective, any event which can lead to customer dissatisfaction or loss of customer faith in the bank is regarded as a threat to the goals of that component and is therefore considered a risk. Similarly, each component of the strategy map is examined thoroughly with respect to its individual goals.

3.3. Risk Assessment

All risks identified are ranked according to its likelihood of occurring and its impact on the financial performance before is classified into risk response matrix. The likelihood of a risk is assessed based on the frequency of estimated occurrence. An event that can occur several times a year or more is considered high likelihood whereas one that occurs less than once a year is considered low likelihood. The magnitude of a risk is assessed based on the tangible effect. A risk which results in direct loss of funds is considered low magnitude. A change in customer preference for example leads to indirect losses and is therefore regarded as low magnitude, since the volume of loss is usually small. A risk which results in immediate loss of funds such as cyber theft or fraud is considered high magnitude since the loss is immediate and usually substantial. The steps taken to manage a risk depend heavily on the interactions summarized in Figure 2.
3.4. Designing a Risk-based Management Control System

This step requires the development of control strategies that would help banks to mitigate risks and enhance their execution strategy – setting of diagnostic control, belief control, boundary controls and internal controls. The explanation of each control is in the table below:
Table 1: Risk management control system

<table>
<thead>
<tr>
<th>Types of control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnostic</td>
<td>Communication of top management’s expectation to their bottom lines and rewards granted if bank employees are able to meet their objective.</td>
</tr>
<tr>
<td>Boundary</td>
<td>Rules in place to limit employees’ activities (i.e. code of conduct)</td>
</tr>
<tr>
<td>Belief</td>
<td>Alignment of organisation goal with employees’ belief and motivation</td>
</tr>
<tr>
<td>Internal control</td>
<td>Effective record keeping and compliance with relevant regulations</td>
</tr>
</tbody>
</table>

4. Results and Discussion

4.1. Perspective Based Risk Identification

Since finance is the core business of any bank, it stands to reason that all risks can be viewed as threats to the financial perspective. As such, it makes more sense to discuss the threats and risks identified from the consecutive components of the strategy map.

4.1.1. Customer Perspective Risk

As the banking sector becomes more integrated with technology, consumers’ are open to a wider range of choices. This will heighten the competition between Internet banking service providers, since consumers are now more informed about their options due to fast and prolific dissemination of information. For example, customers will seek for the best priced loan with the lowest interest rate. The likelihood for this risk is high but its magnitude is low. Although customers do conduct surveys among products offered by different banks, the potential loss suffered by the bank is small as the banks can focus on selling other products.

When initially offering internet banking services, it is of utmost importance to survey the temperature of customer reception before sinking capital. There is always the risk of a lack of reception due to the bank not having established a reputation in the particular region. A good example was the closure of two Internet only Banks (IoB), Wingspan Bank in the USA and FinatiQ in Singapore. With the absence of branch presence, Wingspan Bank was unable to brand itself as a feasible bank (Trombly, 2000). The bank closed down in 2000 after failing to accrue patronage and was later acquired by Bank One. FinatiQ, Asia's first Internet only bank incorporated in Singapore suffered the same fate. The IoB closed down after the management discovered the non-viability of its business model to the demand change of Singaporean consumers (SingWealth.com, 2011).

Aside from this, banks also have the responsibility to always maintain high quality service with minimal disruption and ensure the integrity of customer confidentiality at all times. From the
customer perspective, the events of slow response to customer queries, server downtime, errors in transaction or transaction failures, leakage of customers' accounts or personal details are harmful to the banks goals and result in loss of customer faith and damage to the bank’s reputation. While these events tend to happen fairly frequently, they are not considered high magnitude due to the small impact to a bank’s overall earnings. In a large enough sample population, it would take a very large blunder to catastrophically damage a bank’s reputation and customers do have a certain degree of tolerance to mistakes that involve frustration and loss of time but no loss of money.

4.1.2. Process Perspective Risk

This risk is the most crucial risk faced by Internet banking providers as it affects the heart of their business. Any event which compromises the availability and accessibility of the Internet banking platform or jeopardizes the security of customers’ data and transactions is deemed a risk. Transactional services which deal with fund transfers and registration of bank accounts are the most vulnerable as they are directly linked to the bank’s internal system. Two common factors that give rise to process perspective risk in transactions are cyber-attacks and fraud.

Cyber-attacks give rise to information security risk. The inability to detect the source or timing of an attack increases the likelihood of this risk. Financial regulators and cyber security were also concerned about the high frequency of cyber-attacks globally. NBC News reported fifteen US banks faced cyber-attacks for six weeks that left their system offline for 249 hours (NBC News, 2013). In the recent Sophos Security Threat Report 2013, Malaysia was listed as the sixth most vulnerable country in the world to cyber-attacks for three consecutive months in 2013 (Sophos Security, 2013).
As mentioned in previous section, fraud transactions are a common threat for Internet banking. In Malaysia, fraudulent transactions are commonly caused by phishing attempts, where fake e-mails or short message service (SMS), phone calls were sent to unsusceptible customers prompting them to reveal their personal details and login credentials (refer to Figure 3). Given the seriousness of the issue, fraud is rated to have high likelihood and high magnitude.

Failure of banks’ to improve their processes could also be a major risk to Internet banking business. As technology advances, hackers may find new ways to penetrate the Internet banking system. For example, in the recent case of cyber-attacks on prominent US banks, hackers managed to change the nature of Distributed Denial of Service (DDOS) from a harmless computer bug into a lethal hacking weapon, infiltrating customer’s accounts (Ryan, 2013). It shows that the failure of banks’ to innovate new preventive measures may expose banks to new security threats.

The lack of expertise in the Internet banking area may drive banks to outsource the maintenance of Internet banking service to a third party vendor. Similar to cyber-attacks, the confidentiality, integrity and availability of critical information may be compromised if terms of the agreement signed between vendor and banks are breached. This will lead to incidents of fraud whereby vendors misuse crucial information and conduct criminal activities. Although the likelihood of event occurrence is fairly low in comparison to cyber-attacks (due to vendors already having established chain of commands to prevent incidents such as this to protect their own best interests), the magnitude towards a bank’s profitability is massive.
One notable example is the apprehension of sixteen Citibank call centre Indian personnel for USD 350,000 data theft on April 2005 (Varghese, 2005). The culprits called up four American customers enquiring for their personal login credentials to transfer their customers’ money into their own accounts. Another insider job was reported in Bank of America on May 2011, affecting 300 customers and costing the bank USD10 million (Goodin, 2011).

4.1.3. Learning and Growth Perspective Risk

Technology change is catalyst to higher profitability provided it is managed properly. In order to do so, the bank must possess the expertise and know-how in managing technology related risk. The lack of training or experience in this field may cause slow response to incidental events and it will affect the banking operations. Weak risk awareness in the organisation also affects the learning curve on the latest threats in the technological spheres.

Having poor IT systems can cause significant impact on online banking transactions. Compubank’s case was a clear example of this. The Internet only bank acquired by NetBank in 2001, experienced incompatibility of systems caused by an integration problem resulting in account suspension of Compubank’s existing customer. Compubank’s customers cried foul when they discovered their accounts were inaccessible and in some cases missing funds. The poor response from NetBank’s customer service department worsened the situation, resulting in loss of trust in terms of customers’ perception towards online banking (Lewis, 2001). This example emphasizes the need for good management strategy and sound decision making protocols which incorporate risk assessment and evaluates resource availability before making decisions regarding growth and expansion. It also illustrates the critical importance of good human capital with innate IT expertise especially in the internet banking industry.

4.2. Risk Categorization, Assessment and Management

The threats discussed in the preceding section can be categorized into three distinct groups of risks: information security, transactional and strategic. Each group consists of threats with a similar likelihood and magnitude distribution and are generally meant to be handled in a specific manner.

4.2.1. Information Security Risk

This refers to the threat of a breach in information security processes exposing banks to hacker and virus attacks, data destruction, leaking of clients’ confidential information and fraudulent transactions (Ramakrishnan, 2001). These events often happen in sequences and the perpetrators ultimately aim to manipulate the obtained information to be used as bait to lure unsuspecting customers into revealing account information enabling access to customers’ money.

Often the breach in information security can happen from the customers’ side when they respond to fake e-mails, SMS or other forms of phishing attempts to obtain such information. These attacks occur frequently since they require very little effort and are generally hard to trace back to the source, hence making this risk high likelihood. However the risk is considered low magnitude as long as the information leaked is not critical and does not result in monetary losses. Despite this banks need to be wary of this threat because it is a foot in the doorway to the much more
serious transactional risk. Stringent methods to reduce this risk are therefore warranted. Given the severity of information security risk, banks are required to tighten up their security controls via strong authentication and cryptology for transmission of highly sensitive data (Bank Negara Malaysia, 2010). Best practice to combat unauthorized access is to adopt multi-factor authentication, where combinations two or more factor concepts are used to verify the identity of the customers. These concepts are what you know (e.g. password, PIN), what you have (e.g. one time password or token), what you are (e.g. biometrics) and where you are (geographic location). These mechanisms are strengthened further with the use of cryptology tools such as TripleDES, IDEA and ECC to prevent brute force attacks on customer information (Hong Kong Monetary Authority, 2000).

Besides beefing up security of e-banking platforms, financial institutions must not disregard its end-user as a potential threat. In author’s opinion, any state of the art security controls can easily be overturned by customer’s lack of awareness. Insusceptible clients often get tricked into participating criminal activities being none the wiser (i.e. revealing personal details to unauthorized third party calls or emails).

A probe into Malaysian e-banking fraud cases revealed that clients often fall victim to hoax calls and emails due to gullibility and ignorance towards transaction security (Fernandez, 2010). As such, regulators require financial institutions to play an active role in educating customers on e-banking in forms of awareness campaign and frequent security alerts (Association Bank of Malaysia, 2009).

The Monetary Authority of Singapore (MAS) advocates detailed disclosure of e-banking service to customers informing them about the risks and benefits of using the service as well as customers’ rights, responsibilities and obligation in relation to online transaction matters (Monetary Authority of Singapore, 2008). BNM also embarked on similar mission by having an ongoing consumer awareness campaign organised by commercial banks and Association of Islamic Banking Malaysia in collaboration with Cyber Security Malaysia, the Malaysian Communications and Multimedia Commission (MCMC) and the Royal Malaysian Police force (Bernama, 2013). The concerted effort has successfully reduced the number of fraud cases from 4,380 cases in 2012 to 1,992 cases in 2012 (Bank Negara Malaysia, 2012).

### 4.2.2. Transactional Risk

Transactional risk refers to the threat of monetary losses due to hacking, fraud or other forms of online criminal activities. The difference with informational security risk is very simply the outcomes. An information security risk has the potential to become a transaction risk if preventive measures are not taken. Transaction risks typically arise from cyber-attacks, hacking attempts, fraud or even breach of trust by third party vendors or staff within the bank itself. Besides these brute force attacks aiming to erase data on servers are also dangerous and constitute transactional risks.

Transactional risks are regarded as high impact high likelihood and are a crucial aspect of risk management for online banking. The rule of thumb in managing transactional risk is to ensure financial institutions maintain ownership over critical information at all times (Hong Kong Monetary Authority, 2000). Vendors can only have access to confidential information only if they were granted permission by relevant authorised bank personnel. Activities of vendors need to be well documented in the audit trail for better transparency and reference material during audit processes.
An additional security control is the appropriate review of the competency and performance history of a service provider prior entering into any contract to ensure the vendor’s fitness (Kandan & Idris, 2010). Clearly defined terms on roles and responsibilities of service provider stated in the contract serves as an internal control against any fraudulent attempts. Vendors also need to sign secrecy agreement in accordance to Section 67 in Central Bank of Malaysia Act 2009 as a mitigation measure to protect customers’ privacy (Bank Negara Malaysia, 2010).

Part of the mitigation strategy to reduce transactional risk involves customizable capping of money transfers and seeking authentication at every step to ensure no foul play occurs. For instance, online banking customers in Malaysia are allowed RM3,000 per transaction. Any increase of limit must be done manually over a series of stringent procedures. The bank will issue multiple transaction authorization code (TAC) for each step via SMS to customers as precaution mechanism. If customer did not perform such transaction they can inform the bank immediately. For exceptionally large fund transfers or sudden cash flow movements, systems in place trigger alarms that hold the cash flow until verifications can be made. This alert mechanism is in line with Anti-Money Laundering and Anti-Terrorism Act 2001 to prevent large sums of money from being siphoned out of country in funding criminal activities. However, the detection of suspicious cash flow activities is complicated especially when dealing with business accounts that experience large cash flow movements regularly. The operative mode here however is to err on the side of caution and verify all activity deemed possibly suspicious. These systems are already in place for most credit card transactions but work a little more slowly for small to medium sized inter-bank online transactions.

Having strong organisational culture towards risk also helps in reducing transaction risk. This can be cultivated by setting boundary controls such as code of conduct and standard operating procedures to e-banking employees coupled with effective reporting framework to generate high responsiveness towards transaction risks. This is extremely important given the “no-compromise” policy of e-banking service. Compliance to internal policies not only discourages employees from engaging in moral hazard activities such as stealing clients’ information from servers but also encourages alertness to suspicious behavior and consequently faster and more effective detection and countermeasures.

For transaction risks deriving from vendors or third parties, the general method of managing the risk is to transfer it to the vendor in the form of insurance or other forms of legal protection. This way the vendors are entirely accountable for glitches occurring on their end thus making the risk manageable for the banks.

4.2.3. Strategic Risk

Strategic risk refers to improper implementation of business strategy resulting in negative effect on banks’ earnings (Ramakrishnan, 2001). This risk may arise when product offerings do not match customers’ preference or inflexible internal capabilities (talent and equipment) result in failure to provide high quality services. As a result, financial institutions may incur high sunk costs if investments made in hardware and software is not compatible with the brisk change of technological advancement.
However, the author believes that the likelihood strategic risk is low because of strong corporate governance in financial institutions. Similar to other critical areas of banking, the decision to pursue provision of e-banking service has to go through rigorous evaluation process before final decision is made by the Board of Directors. Moreover, financial regulator like BNM also requires banks to submit their business proposal for approval prior launching their product to the market (Bank Negara Malaysia, 2010). This requirement is to provide check and balance mechanism to ensure the viability of banks e-banking strategy. Therefore, the likelihood of wrong decision made is very slim.

E-banking providers also have business continuity plan in place to mitigate any possible disruption. Banks such as CIMB established disaster recovery plan (DRP) where an independent IT service provider stores critical information in servers maintained at backup site at a different location (CIMB, 2007). This will ensure instant recovery in event of operational failure (i.e. server downtime). Financial institutions also established robust monitoring framework and reporting system to keep the management abreast with the latest development of technology. This knowledge will help them to make informed decisions and set their risk tolerance related to e-banking.

Essentially strategic risks have low likelihood and high magnitudes. As such, these risks need to be mitigated and controlled through good management and planning. Decisions made should be based on empirical evidence instead of optimism alone and some funds need to be invested into research and development to ensure banks stay ahead of the IT learning curve.

5. Conclusion and Recommendation

Online banking is a risky business due to its innate association with large amounts of money, thus attracting frequent criminal activity. However with good risk management this business can be extremely profitable in the long term. The three groups of risks identified: informational security, transactional and strategic risks are each handled differently based on their assessed danger.

Information security risks which are high likelihood and low magnitude must be mitigated using multi-factor authentication, encryption and education to raise consumer awareness of fraud and unauthorized information requests. These measures must work in tandem with detection and countermeasure protocols to minimize occurrence of transaction risk.

Transaction risks which are high magnitude with variable likelihood need to be either transferred or avoided. In the case of third parties or vendors, the risk is transferred via a legal process which holds third parties responsible for safeguarding information in their possession. However, avoiding cyber-attacks and fraudulent attempts is a much harder process which involves multiple checkpoints and verification or authentication along the way.

The best way to reduce transaction risk is to pre-emptively hold or check any suspicious activity which calls for a complex monitoring system with fast reaction towards risks. Finally strategic risks are managed with the use of standard operating procedures and protocols, benchmarks and regulator surveillance.
This study suffers from one inherent deficit in that all risk and mitigation methods are derived from various guidelines from banks. This is because of the nature of this information which is highly classified and the extreme lack of resources related to this field of study. The lack of real working knowledge of online banking operations is somewhat alleviated by the sheer size of literature backing this paper. However to improve this study, surveys or interviews of banking personnel to gain deeper insight into the risks involved in online banking and more specific solutions and remedies to each risk.

While the current measures of risk management employed by banks are deemed sufficient, the author recommends that banks should gradually move towards internalizing all critical processes involved in online banking. This would mean cutting out the middle man or in this case, third party vendors by training bank personnel to be IT proficient and owning and managing dedicated servers. The advantage of this would be the removal of many links in the chain of command and creating a smoother operating process with greater accountability and transparency.

From a financial perspective also, this is beneficial on the long term and a preferable solution to outsourcing. In line with this, banks should seek to upgrade their respective IT departments to not only solve domestic hardware and Wi-Fi connection problems but dedicate a specialized task force to research and develop better firewalls, interlocks and security measures for safer online banking. Such a team should also be the first to be notified of cyber-attacks and investigations into recent threats should be conducted by them.

Finally, this team should be consulted before any relevant strategic decisions are made to ensure congruence between capabilities and management goals. In short, it would behave banks invested in online banking to acquire the technological savvy, human capital and equipment currently owned by third party vendors in order to achieve long term goals.

References

[Accessed 22 April 2013].

[Accessed 14 March 2013].


[Accessed 11 March 2013].


