Information Security Risk Management in Electronic Banking System

U Sai Saw Han
Faculty of Information Science
University of Computer Studies (Myeik)
Myeik, Myanmar
saisawhan@gmail.com, saisawhan@ucsy.edu.mm

Abstract

Information and communication technology stands up as an important and effective part of various organization in Myanmar. By use of telecommunication network and internet, the information security and IT risk management system become indispensable requirement of organization. The organization need to maintain their information from when internal or external threats are incident. All of threats might control the information security risks and organizations are managed their own information environment. So, the organization required that they maintain and cover with high level security system. This paper focuses on information security risk management in the some activity of electronic banking system (e-banking system). The electronic banking technology is allowed for a variety of implementing financial services between organizations and customers. It allows serving, business market to improve customer service all the time [3]. The use of e-banking system is high rate in developed countries and comparatively lower in less developed countries. The analysis of the evolution and existing standard of electronic banking made the economic opportunity grow for the government [4].

Keywords: *E-banking services, security, risk management*

I. Introduction

All organizations must have information security model and it is a resource or information to be protected and kept safely. Assets, vulnerabilities, threats, and controls are the basic requirements of information security model. E-banking (Electronic banking) technology is popular in Myanmar banks. It a means of communication between computer system and information communication technology to archive many benefit for customer and bank. There are a total of twenty eight local banks and thirteen foreign branched banks in Myanmar. Including five organizations authorized by the Central Bank of Myanmar to provide mobile financial services. The way for customers to interest with banks, E-banking channel, such as online banking channel, mobile banking channel self-service terminals, social media platforms and mobile payments channels are very interesting. Many banks in Myanmar have long offered e-banking services for customers to perform online balance enquiries and fund transfers need to solve the requirements to assess customers' compliance [3].

By the increasing use of mobile devices and social media platforms, banks depend on the requirements of technical and controls corresponding e-banking service system platforms have been enhancing their existing e-banking system platforms to improving their mobile banking application system and functional platforms. Professional responsibilities of information security professionals include a mix of technical and nontechnical activities. Their technical responsibilities include planning, implementing, upgrading, or monitoring security measures for the protection of computer networks and information. It is important to identify asset that are need to be upgrade process in developing technology and potential risks with e-banking system and so that the organization can deploy the right controls across the banks. The challenge is to determine what needs to be protected. By means of assets manages by IT systems, which have one or more vulnerabilities. Adversaries are interested in exploiting these vulnerabilities by means of threats. Information security professionals use control to ward off these threats.

In developing mobile technology and the potential risks associated in present, the system need to be upgrade process a wider scope of e-banking process. The new requirements shield of online banking, mobile banking, self-service terminals, e-banking services in social media platforms and contactless mobile payments detail depend on the technical requirements and controls corresponding to the provision of e-banking services. Much of new risk management are required to solve and guide customer complain. The weakness of the requirements for banks has an extended scope of e-banking. Banks will need to perform an overall review based on the new to ensure compliance with the extended scope of requirements. In the technology control standard of the industry improving technology risk and actively issued adapt increase regulate on cyber risk and technological risk. Banks are used this process to assess the benefits carry by e-banking channels and improve upcoming technology strategy and way [3].

The other researchers work related in e-banking system are top point out the risks of e-banking which both banks and their clients face all the while placing special attention on examples of risk management of electronic banking and security challenges in e-banking. The objectives of this survey analysis are to understand the impact of e-banking on the banking performance, to know the various risks and security challenges in e-banking, to manage the risk and security aspect of various e-banking services where customers have high level of concern and to get knowledge of the e-banking and its impact on traditional services in less developed countries.

II. E-BAKING AND SERVICES

E-banking is providing to twenty four hours access available at every time for whom with the customer contact. It can reduce waste time to visit to check information of balances or transferring money to another as in normal bank. Because of low operating costs of e-banking came into existence in greater numbers of the usage of e-banking by the enterprises now. E-banking transaction service is based on information technology and it can provide financial transactions electronically fund process faster services and low cost between banks and customers. Automatic teller machines are start of developing banking process and it developed to internet banking services done in mobile devices become used of the best financial transactions. It can use easier and banking process faster between customers and banks. To perform financial transactions by use of card, the electronic payments and where the cardholder pays by using of computer systems. There are many transaction types such as deposit, withdrawal and electronic fund transfer to account. To protect non-financial transactions, the administrative that including identification number is needed. During e-banking procedures the electronic funds transaction need to be activated. TV banking, short message service banking, mobile banking and internet banking system are useful types of e-banking system. For customer to access financial service an internet connection is required. E-banking remove the customer personnel activity in e-banking system, the service transaction to provide the benefit depend on customer responsibilities. Thus, to fit the process the customer require knowledge, understanding the technology of the banking system and interface.

In development of mobile technology, mobile software is a program that downloaded onto a mobile device or accessed by a device used of the internet. The use of mobile device for financial transaction service need to understand the sequence of instruction. The knowledge of the risks and experience of customer are limited. The mobile banking applications (online shopping systems, mobile payment systems, mobile banking system, mobile play store and so on) are applications that can be used by mobile devices that allow to browsed complete customer wish and banking transactions process. Mobile accounting, mobile service fee and user financial information are the three main parts of mobile banking system. Administer managed to operate of the account in mobile accounting services. Mobile accounting services have account operations and account administration. Account operations are services for fund transfers and bill payments. Account administration manages by blocking lost cards, update active accounts, and instruction to check. Mobile service fee are the services that are required to benefit for an investment account, including the variety of funds operation and requirements of information securities. Account financial information and market target area are the main part of mobile user financial information services. Account information includes information of balance inquires, requests, alerts, location of branch, and veritable card information. Target area information provides information played exchange rates, interest rates, products and services information. Many banks in Myanmar have mobile application that allows to taking online banking application in mobile devices. It more convenient and quickly checking up to customer account information and funds transaction.

Every bank has system architecture for managing the operation and security risks depend on system design and control processes. Bank also need to be update and the staff require training to new system architecture for bank efficient service. The important critical issue for banking system is reputation. The common type of risk in e-banking is transaction risk. Because of incorrect processing, data integrity compromising and by access of unauthorized to system the transaction risk can occur. The missing authorization vulnerability happens when a software program allows users access to privileged parts of the program without verifying the credentials of the user. This vulnerability is particularly harmful in the financial industry. Attackers are always trying to find parts of financial information systems that they can reach without credentials. For example, according to the "top 25 dangerous errors" publication, hundreds of thousands of bank accounts were compromised in May 2011 at Citigroup as a result of missing authorization vulnerability [1].

The process of risk management and implementation of business objectives are important in information system.

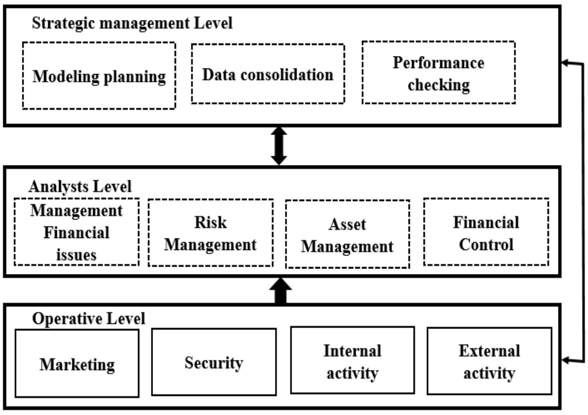

Figure 1. Architecture of Banks' information management system

This system structure is included three levels of organization, which are strategic management level, analysts' level and operation level of organization which can be seen in figure 1. The way of efficient transferring information between management level and strategic management level can be easy to achieve goals and operation process including the expert's field of risk management, analyst state to offer solutions in banking operation. The middle of management specific set of goals and recreate the specific issues.

III. SECURITY OF MOBIL-BANKING

Today mobile communication becomes network connector of the human society. Mobile banking system is one of the most useful applications in mobile communication system. The information security is an important part in mobile banking system between customer and banks. The information security in mobile banking system is be as follows:

A. Information distortion and damage

Mobile communication system is used wireless transmission media the modulation process need to convert analog data to digital signal modulation techniques. In mobile communication network technology provides limited tools to cover the transmission media. Attacker can modify the information to distortion or damage the used of legitimate users the overlapping and installation acceptable in mobile communication network and then modify or update data or delete. Confidential banking information may be weak and distortion damage in the daily transaction devices [4].

B. Incomplete process information

If a customer use mobile device in poor of communication network connection it will be become unwanted data processing and incomplete communication information. Delay or failure transaction can occur in interruption by noise or other signals. It lead to unfinished transaction process could be easy to incomplete data or loss. Banking organization need to turn off and make the information unfinished.

C. Virus attacks control

Target of hackers is the weak of e-banking and security is one of the risk management problem by customer in access their account using internet. An intended as an attack have plan to the system fraud. Living in digital age, despite the current virus on mobile operations found mainly destruct mobile phone function, use of mobile phone application, restore the battery of charges, log on to using internet and record other data are all faced with the threat of exposing private information [2]. The virus designed to do harm to mobile system, replicated and infected to operating system and spread to other system. By the passwords control, firewalls and antivirus software control are built into the information system itself by technical controls [1].

D. System and data integrity

E-banking systems are more available than Traditional banking system. It can provide internet access for their customers with paper less system. A customer can print the information by using internet. It provides the relations and satisfaction able to create. If a customer does not want to use e-banking system, the system may be break and cut available services to a customer wished in bank. E-banking system allowed to customer the control and manages in his account. The integrity process of the system allowed testing and documentation to complete of banking system.

E. Digital Signature

By means of digital signatures based on encryption and decryption method technology which built solution with signed document verified the authenticity of signed record. It plays a role in the data authentication and non- repudiation.

IV. CYBER SECURITY RISKS

Cyber security risks in e-banking systems are corresponding to using of internet. Cyber security in an organization is used of technical infrastructure to protect data and information from cyber-attacks on e-banking system. Source of cyber risk can meet, the organization reviews to manage the weakness of issues and IT function cover to multi-level of cyber risks.

The following resources are the key areas that organizations should look into when incident of cyber risks.

1. Leadership and governance
2. People factors
3. Information risk governance
4. Business management
5. Operations and technology and
6. Rule and law

A. Leadership and Governance

Maintenance and development of the e-banking system depend on the technology and responsible in department of organization. E-banking system with build in designed, infrastructure of process and procedures. That have to be responsibility in e-banking system to obtain manage the procedures of reasons in nonfunctional conformance policies. The departments need to develop and manage the risk of requirement. If necessary to assistance formulation and procedures should checks the adequacy existing controls management.

B. People Factors

All of employees in an organization have the various knowledge and expert in their job. The responsibilities of senior management in e-banking are abide in security and banking strategy. By using IT to handle not efficient manage to organization them self. To improve the weakest of cyber security in people, training the staff to improve knowledge and understanding help are the effective ways.

C. Information Risk Governance

The requirements of evolution continuous corresponding to the risk management in organization depend sample review the procedures and policies of system. That identified requirements of risk assessments on e-banking system sample document and result in the risk. Documentation procedures and policies performed required activities. In use of different e-banking frame, the requirements and industry achieved the good banking policies in time by time.

D. Bank Management

The process of managing the bank’s activity refers to bank management. It is financial relations connect with bank activity and management function in implementation of banking system. The application infrastructure support to target areas that are with a view to get profits and recovery plans should failure of other technical issues. The operation management for organization is to manage daily improves all over the customer.

E. Operations and Technology

The development of internet technologies with new processing of frame including mobile banking, online banking and media form submit to web site. The risks occurrence in banks, it is associated risk assessment to step by step to design banking frame. The weakness of cross channel risk assessments is the one of the common factor in regarding e-banking system. The impact arising from other banking system for bank to comprehensive is important for cross channel to understand on banking system. Mobile application updates are software updates that fix activity with components of the application software. The system directly developed and released by software and it automatically checks for installing or updates system administrator intervention.

F. Rule and law

E-banking system determine to perform normal risk assessments on existing banking system is required. Compliance departments work in financial services activity meet for efficient, transparent and markets are fair. The documentation is reducing system risk and financial crime. The independent assessment is needed to decide the various technology requirements in internal or external consultants to generally review their requirement and compliance.

V. Methods

A policy is a document that records a high-level principle or course of action that has been decided on. An information security policy therefore records high-level principles on information security that have been agreed on at the highest levels of the organization. The goal of an information security policy is to obtain endorsement at the highest levels of the organization for information security activities. Policies are written in a language that is general enough to deal with routine developments in business and technology. While a policy specifies a general direction for the organization to follow, without concerns for how to get there, standards, guidelines, and procedures focus on how to get where the policy desires to go [1].

Risk is a quantitative measure of the potential damage caused by a specified threat. We may write this managerial concern as:

Manager’s decision problem = max (profit) or
Manager’s decision problem= max (revenues – cost)

At the very high level, risk management can be known as the management the financial impacts of unusual events. To modify the manager’s decision problem as:

Max (Revenues – cost – Δ),
Where Δ is the impact of unusual events on the organization.

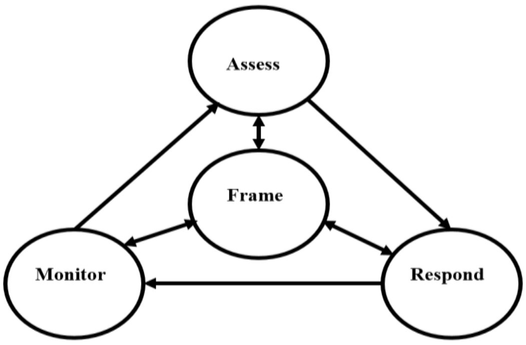

Figure 2. Risk management framework

The risk frame, the risk assessment, the risk response once the risks are assessed and ongoing risk monitoring based on the experiences are the four components of risk management framework show in figure 2. The frame determines the risks the organization focuses on. The assess stage quantifies the risks in the risk frame. Monitor and respond involve managing the assessed risks. A framework is a structure for supporting something else. In the management literature, frameworks are used when a large number of ideas are to be organized in a manner that can be understood and memorized by many people. The objective of framework is a recommendation for managing information security risks. The identified organizational risks can include many types of risk. The risk frame establishes the context for risk managements by describing the environment in which risk based decisions are made. IT risk management is the assessment, monitoring and response to risks associated with the use of information systems in an organization [1].

The IT risk frame establishes the context for risk management by describing the environment in which risk-based decisions are made. The frame clarifies to all members in the organization the various risk criteria used in the organization. These criteria include assumptions about the risks that are important, responses that are considered practical, levels of risk considered acceptable and priorities and trade-offs when responding to risks. Risk framing also identifies any risks that are to be managed by senior leaders/executives [1].

During in (2018 June to December) the past six months, efforts by KBZ Bank staff across the country bring one millions of people to the mobile-friendly economy. KBZ Bank aims to reach 30 million KBZPay users over the next ten years, as mobile population growth in the country increases [7]. Because of the average of over two thousands KBZPay customers increase in monthly by Kanbawza bank (3), this research is used of case study based on analysis of information risk management in banking. The optionality question are designed to analyze the risk associated with in the banking sector. The user option are paper form and administered to local zone in University of Computer Studies (Myeik) in Myanmar. The total number of 135 students including employee respondents was achieved.

The five scale rating structure system includes rarely option, never option, very frequently option, frequently option and occasionally option. In order to obtain the risk impact associated to options as contained in the administered optionality. The marge of rarely and never option values indicate the high risk impact, the associated option values show medium risk impact and the marge of very frequently and frequently option vales indicate low risk occur [8].

A. Results and Discussion

This research state that 28.15% are male and 71.85% are female respondents. It indicate the most of respondents banking user of female are more than male banking user because of female students and employee more than male show in figure 3 below.

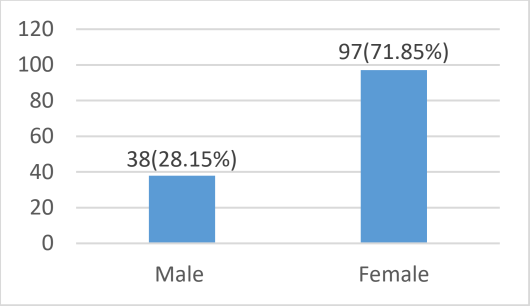

Figure 3. Gender distribution

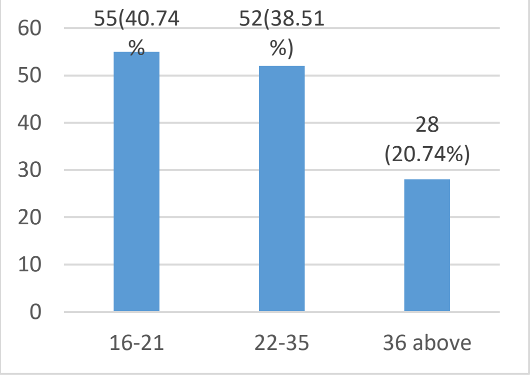

Figure 4. Age distribution

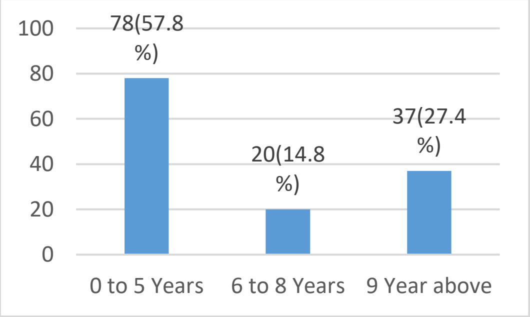

Figure 5. Banking experience

Figure 5 state the experience in banking system, 57.8% have under 5 year experience, 14.8% respondents have 6 to 8 year experience and 27.4% respondents are with 9 year above. This indicate all respondents with a good period of time in banking system.

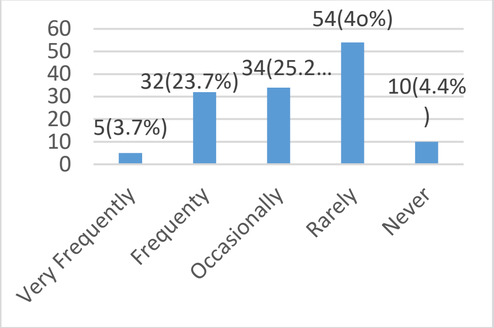

Figure 6. Confidentiality level frequency of KBZ pay and ATM

In above figure 6 states the ATM (Automated Teller Machine) card and KBZ pay account exposed 40% of the rarely live their account, the respondents occasionally leave 25.2%. The frequently never used with 4.4% and 23.7% respondents never leave their account and card. 3.7% of the banking user leave their account very frequently. 21.48% respondents are occasionally.

The figure 6 shows the state of seek for assistance during an online transaction. 62.9% of respondents no need to seek for online transaction, 17.1% occasionally seek for assistance and 20% of respondents seek for assistance.

In figure 7 in below showed 31.85% respondents used their devices in financial process frequently and 29.63 very frequently. 21.48% respondents are occasionally and 17.04% respondents are rarely used their device in financial transaction.

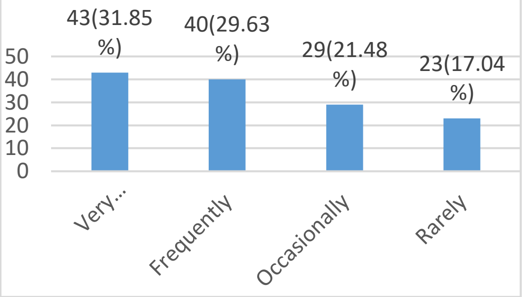

Figure 7. Frequency used of smart devices with password in financial transaction

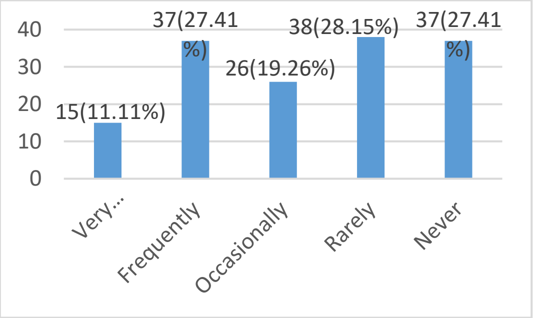

Figure 8. Frequency of free wireless access point used for online transaction

In figure 8, it shows the use of wireless access during in online transaction. 28.15% are rarely use wireless access point, 19.26% used occasionally, 27.41% respondents are never use free wireless access point in online transaction, 27.41% are frequently used and 11.11%respondent very frequently use wireless access point for online transaction.

According to figure 6,7, and 8 in this survey, that exposing ATM Card or KBZPay will have a high impact of risk on the customer, while sharing of ATM Card and PIN with third party also has a high impact risk on the customer, while the necessary of devices using password for online transaction and having a licensed antivirus software with on the devices used for online transaction indicate a low impact risk, during online transaction, using a free wireless access point and been debited without a successful transaction all have a high impact risk on financial institution.

B. Suggestions from Survey analysis

1. In e-banking system construct by one of supervisory policy manual and other monetary authority hold together with two factor authentication services, account unity response services from when the threat is incident and so on. The customer compliance of requirement is solved by banks. Banks need to examine to the e-banking services in supervisory policy manual.
2. The board of organization and senior managed to e-banking system when the incident of risk occurrence and including employee resource. The requirements of adequate employee skills are depend on expertise senior management to manage the risk. Accounting staff manage e-banking services for specify of banks.
3. Fund transfers to unregistered third parties are considered high-risk transactions and should be subject to two-factor authentication. Small value fund transfers to unregistered third parties can be performed without two-factor authentication. Banks should refer to the requirement stated in the additional guidance on SPM (Supervisory policy Manual) also consider the banks' own risk appetite when determining the caps for small value fund transfers [3]. In two factor authentication, the fund transfers to without accounting person to performed risk transaction. It can be performed by banks should supervisory policy manual to manage the risk, bank also determining to allowed for few value of fund transfers.
4. Application forms are not required in online. Banks are needed to solve to assess the risk and establish controls the online services information. The required of service include:
   a. The use of password to protect the confidentiality and integrity of the information sub-post to online.
   b. Manage to cyber attacks through the documents information.
   c. If required, checks to rule identity of the customer online services information [3].
5. In mobile banking system, the security and weakness of mobile application specific risks and banks also need to assess the detail risk and management to mobile banking infrastructure. Many risks can be asses in attacker attack, risk from virus, structure of security and devices loss of customer.
6. Including the weakness of credit card information and transactions process run in mobile devices, banks need to assess security risks on contactless payments and defined multilevel security risk. The standards of security issued depend on banking associations and mobile payment services are ensured in banks sector.
7. The notifications system is important part of the maintaining and solving the process of system implementation. Banks always need to promptly customer requirement notify transactions include card damaged or other. Banks need to solve immediately by using automated process after detection notify high risk transactions occurs.

VI. Conclusion

Many organizations use information and communication technology. For developments of any organization (such as business, financial, database record keeping and so on) are needed to manage information security and risk management system in organization. Especially, many banks in Myanmar use information communication technology. Every banking system to fulfill the needs of the customers in managing their personal information, data, and security. The e-banking technology is allowed for a variety of implementing financial services between organization and customers. Because of mobile banking system is attractive and convenient to perform remote banking approached, the improving information security risk management in e-banking system, it can useful tool of system development and main issues of mobile telecommunications technology especially mobile device function improved [4]. It can integrate the mobile banking and current service. In banking industry, it make easy use of the benefits provided by of mobile phones and develop a unique customer oriented services will be stand to play more standard role. The main challenges in e-banking system are it has run and developed for different operating systems of mobile device and on security issues which has the risk to the customer who use mobile banking system.

REFERENCES

[1] Eric Pierce, Alex Campoe, Manish Agrawal Information Security and IT Risk Management

[2] Walfried M. Lassar, Chris Manolis, Sharon S. Lassar (2005), “The relationship between consumer innovativeness, personal characteristics, and online banking adoption", International Journal of Bank Marketing; Volume: 23 Issue: 2; 2005 Research paper

[3] Henry Shek, Kelvin leung. “Internet Banking Update, The New Electronic Banking and Cybersecurity requirements”

[4] Jin Nie, Xianling Hu. “Mobile Banking Information Security and Protection Methods” 2008 International Conference on Computer Science and Software Engineering, 2008

[5] https://www.cbm.gov.mm

[6] Dugguh, S.I.,PhD& Diggi, J. (2015). Risk Management Stategies in Financial Institutions in Nigeria: the Experience of Commercial Banks,2(6),77-73

[7] https://www.kbzbank.com/mm/

[8] Noah N. Gana, Shafi’i M. Abdulhamid, Joseph A. Ojeniyi. "Security Risk Analysis and Management in Banking Sector: A Case Study of a Selected Commercial Bank in Nigeria", International Journal of Information Engineering and Electronic Business, 2019 Publication