LAUREA
AMMATTIKORKEAKOULU
Uuden edellä

Security analysis of online banking in China: A Case study of the Agricultural Bank of China

Wang, Anqi

2014 Leppävaraa

Laurea University of Applied Sciences
Laurea Leppävaraa

Security analysis of online banking in China: A Case study of the Agricultural Bank of China

Wang Anqi
Degree Programme in
Business Information Technology
Bachelor's Thesis
May, 2014

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaraa
Degree Programme in Business Information Technology

Wang, Anqi

Security analysis of online banking in China: a case study of the agricultural Bank of China

Spring 2014 Pages 44

The rise of online banking has been accompanied by an increase in associated security risks. This thesis examines the various means of protection available to the consumer in order to provide more information related to securing online banking for customers.

Online banking represents a new business model and development direction. It brings changes to banks by decreasing fixed branch and operating costs, and provides an uninterrupted 24-hour service for customers. The most profound changes are that banks must change their role from that of intermediary agency that manages financial products to service institution that provides information about investment and financing. This is not only a major change in operation principles in the financing industry, but also the trend of development of the financing industry in the age of the network economy. However, with the advent of network technology, online banking brings various risks as well. Therefore, a security analysis of online banking is beneficial for operating its business.

The Agricultural Bank of China is a popular bank with many branches across China that maintains an online banking presence. Presently, its online banking technology and banking business are in a leading position in the domestic trade. The online banking service of the Agricultural bank of China is selected preferentially as the online payment tool by many well-known e-commerce sites. Online banking of Agricultural bank of China as a case study is conducted to investigate the security analysis.

Key words online banking, system security, system risks, online payment, Agricultural Bank of China

Table of contents

1 Introduction

In recent times, the use of online banking is rapidly increasing around the globe. This study focuses on online banking and related security situations. This is a case study of 'Agricultural Bank of China'. This working life project has been part of my bachelor thesis work. This chapter presents the introduction and problem discussion of the study at hand. In addition, it defines research questions and the purpose of the study. The introduction describes the background of online banking and out case. The factors for studying on this topic and then briefly demonstrate-how it develops in China? Furthermore, it describes details of this development leads to the security challenges. This chapter concludes with outline of thesis structure.

1.1 Background

The information technology revolution has achieved a profound and lasting influence for human society, and while the emergence of the Internet brings a qualitative leap to the human life, it has also brought a revolution to the financial industry. The establishment of online banking gives commercial banks a platform to create an advantage in banking services, and through such a plat-form commercial banks have formed a borderless development space unlike any other business or estate in the whole financial service industry (HR-Focus 2000). This breaks the hold that branches can have on business expansion and extends the financial service from visible reality to the invisible digital world.

As a combination of information, capital and logistic flow, the e-commerce cannot operate without the support of online payment. Thus, objectively the development of e-commerce requires the banking industry to develop the online service simultaneously to ensure the capital flow precisely and safely on the Internet in order to realize the purpose of the e-commerce. And the basic approach for the bank to accommodate the e-commerce is to develop online banking.

The fierce horizontal competition is the inevitable choice of online banking development, to survive and develop during the competition, any bank that unwilling to be left behind shall have enough internal motivation to develop its online banking, utilize the internet to discover new banking business become a new frontier which each bank will compete for (Reichheld et al. 2000).

1.2 Problem discussion

The Chinese banking system has been through a dramatic change since the beginning of the economic reform in 1979, during which information technology played a major role upgrading

banking services in China As one of the most prominent contemporary banking service, online banking brings customer much convenience as well as potential risks. Online banking insecurity may cause customer's distrust to online banking services and such influence may even spread to the whole banking system. Recently, dramatic development of online banking within China result its common acceptance in society. However the nature of potential risks of online banking with combination of the contemporary condition of China shall draw great attention to avoid severe risk damages.

As a leading bank in China, the Agricultural Bank of China (ABC) has sufficient experience and appropriate precaution mechanism against online banking risks which one may learn from. Agricultural Cooperative Bank established in 1951 as the predecessor of the ABC and has transformed into three stages which are owned by state specialized, wholly owned by state commercial, and controlled by state commercial. In January 2009, the Bank was changed their company type as a joint stock limited liability. And in July 2010 the Bank completed its transformation into a public shareholding commercial bank. The Bank strives to expand its market internationally and to provide its customer with various services in order to being a too-ranking commercial bank in the morden and internationalized world. According to the ABC website report, the ABC utilized the combination of businesses, through developing widely distribution and IT network field to expand the scope of their business for all kinds of corporate and individual customers (2014). Investment inside bank, management of fund, financial leasing and life insurance are included in the scope of business. The Bank's total assets approximately RMB 13,244,342 million until 2010. And RMB 10,862,935 million deposits and RMB 6.433,399 million loans included in total assets which present the good development in these years. The net profit achieved in 2012 was RMB 145,131 million. (Agricultural Bank of China 2014.)

Online banking security is still remained as a major focus for the ABC. The study at hand aims at investigating online banking characteristics with regards to its development and bearing risks in a Chinese context. By learning merits of the ABC and identifying its risks, a better online banking solution can be provided to customers as well as other banks.

1.3 Purpose and research questions

The purpose of this study is to examine security of online banking of the ABC. In order to obtain an in-depth understanding of such issues the author would conduct the study by put up two research questions:

RQ1. What are the factors that bring risks to online banking security of the ABC?

RQ2. What protection methods are adopted by the ABC in order to reduce the risks?

1.4 Structure of the thesis report

In order to help readers better understand the study at hand, the following table presents how the study is organized.

Chapter	Content
Introduction	This chapter demonstrates an introduction including the background, problem discussion, and purpose and research questions to this thesis.
Literature review	The purpose of this chapter is to give the literature review to the thesis.
Research methodology	This chapter describes the specific research methodology including research approach, research design, research strategy, data collection, data analysis and validity and reliability, related to this thesis.
Empirical case	This chapter presents the case in detail from the data collection and interview.
Analysis	According to combination of research methodology and empirical case, the analysis of this case will be presented as two aspects: risks and precaution.
Conclusion	The result and suggestion of this study will be discussed and concluded in this chapter.

Table 1: Structure of thesis report

2 Literature review

This chapter will demonstrate the theoretical background of this study. This theories regarding security issues mainly include two fields: network security and online banking in China. This two therioes will lay a foundation for the later research study such as data collection and data analysis in this thesis.

2.1 Network security

The foundation for security analysis of online banking is the security analysis for network. Online banking maintain their security level on network security level. Network security plays a pivotal role in supporting and improving the development of online banking in security performance aspect.

Network security means the hardware, software and data within network system is protected and system runs continuously, reliably and normally without damaged, modified and leaked for accidental or malicious reasons. The network administrator controls the network related to the data can be accessed by authorization (Network security 2014). Network security includes network equipment security, network information security and network software security. Generally, the technology and theory involves confidentiality, integrity, availability, authenticity and controllability of information on network are all belong to the research field of network security. It is also divided as public and private computer networks, which used in business transaction and communication among enterprises, government institutions and individuals (Network security 2014).

Network security contains three critical elements: prevention, detection and response. These three elements combine to decide the whole effectiveness of security system (Krawerk 2006, 6). Prevention addresses the procedures eliminating an attacker or mitigates a system compromise. Such measures include physical network architecture, firewall elements, antivirus systems as well as system hardening and user education. Although an environment, which solely relies on preventative measures, may be difficult to compromise, a compromise may create an extreme impact. For example, a home computer, which follows an antivirus system protection strictly, may benefit from the antivirus system as most antivirus systems use signatures to identify known viruses. However these signatures may not be updated all the time and the antivirus may fail to identify the new viruses. As the user relies so much on the antivirus system and may not notice the infection from the new virus until it is very late and the important information becomes theft. Being different from prevention, detection functions in the way that is beforehand prevention. Detection is to provide step toward responding to the threats when it knows a system is under attack even if the attack is an ineffective one. These different types of network analyzers act as Intrusion Detection Systems (IDS), which use signature-based systems on a basic level similar, like antivirus signatures (Krawerk 2006, 7). An advanced IDS bases its implementations on common network usage patterns and identifies unexpected network activities. The identification of unexpected network traffic or new network patterns provides an early warning system and allows a defender to have time to quickly take response to an attack. Though prevention and detection systems may collocate in a good manner, a determined attacker can still somehow manage to compromise a system. Then the response system needs to take actions including removing access control, backup devices, and

most importantly, response procedures. Responding to a compromise is as important as identifying the compromising.

Attacks may be internal, external to a system as well as intentional or accidental (Krawerk 2006, 8). Thus understanding the likely vectors and possible motivations of attacks will facilitate the address of security needs, allocating of resources and etc. According to a survey conducted by CSI Institute and FBI, the risk from internal attackers is nearly equal to the risk from external attackers. Meanwhile the damage caused by insiders in dollar value is dramatically greater comparing to the external attacks. Internal people possess better knowledge of the targeting systems and know how to best attack them. There are several reason causing internal attacks such as personal issues, unfair disadvantage, greed, curiosity, ignorance and etc. The damage caused by insiders includes theft, vandalism, information leakage, destruction and so on (Krawerk 2006, 9). The simplest way to protect against physical damage such as theft and vandalism is to monitor they system. While the best way to protect system information from sabotaging is to do backup and to limit access by setting restrictions. External attacks are usually resulted from political, status and power issues. The attackers may use the attack to demonstrate his technical superiority or to simply make a statement. In some cases, external attackers and internal attackers even collaborate and bring disastrous damage to the system.

According to Krawerk, there are five basic concepts forming the foundation of risk management: confidentiality, authentication, authorization, integrity, and repudiation. Without every single area of a system strengthen, the system can still be positioned in a potential vulnerable scenario. For example, bank ATM systems allow users to use PIN numbers for identifying and granting access. PIN supplies authorization but it may be not supply integrity if the PIN is stolen or confidentiality as people can see you at the ATM. Confidentiality implies the ability one operates in private. Authentication is the principle for one system determining the origin of another system. It is essential for an online community. Authorization and access control offers different level of access accordingly to the level of user group. ID, badge or key authentications are commonly sued methods to differentiate access level. Integrity is the prevention of information being either tampered or modified. Nonrepudiation is to make sure an originator cannot falsely repute information. (2006, 12-13.)

Several basic approaches for mitigating security risks are developed to proactively limit the impact from a security breach regardless of the environment (hardware, software, network, and physical). Krawerk (2006, 14) presents that compartmentalize is the simplest way to mitigate the risk from a multifunction system failure by separating out the functionalities. These functional units are integrated into a large system. While the failure occurs in one of the component, it may reduce the functionality of the large system, but the failure would not

negate the functionality from the other unites, which means the scope of the failure is limited to the least. Secure fail happens when a failure occurs, the impacted united should securely fail without increasing the threat level in terms of spreading failures to other units. Defense-in-depth means employing tolls and services from multiple vendors and generating more security. The security level will be increased due to double-check, triple-check procedures, it increases system complexity and compatibility. For example, a network with three virus scanners may prevent 99 percent of computer viruses, however the cost of maintenance will be tripled (Krawerk 2006, 15). Security-by-obscurity is the concept that denotes any mechanism is only secure when attackers are lack of knowledge. There is a common misconception with the software development community that there is a trade-off between security and usability. The higher the security, the more usability will be sabotaged by it. This is only true in some extreme cases. Usability shall not be strictly referred to restrictively functionality (Krawerk 2006, 17).

2.2 Online banking in China

The purpose of this chapter is to provide the theoretical background of online banking. It describes that the definition, the related security issues, the characteristics and general risks of online banking. Finally, the current status of the development of online banking in China is presented to provide the corresponding information for the thesis.

2.2.1 Definition

As traditional banking business hour is very often in collision with customer's time, the invention of online banking can solve this problem by transforming banking business through e-Business through utilization of various e-Channels. According to Milutinovic and Patricelli, Internet, WAP based mobile network, ATM network and web TV and etc. are belong to e-channels which could allow to process the transactions without the regional and time limitation. (2002, 85.)

2.2.2 Security issues

Online banking relies on a networked environment where a computer network is simply arranged with multiple computers with shared information, application, and equipment. The design of networks is for the purpose of increasing efficiency, convenience and access (Milutinovic & Patricelli 2002, 87). Therefore network can be accessed through a combination of devices such as personal computers, cellphones, interactive TV equipment and etc. Various accesses to the network expose the network into the danger of being jeopardized internally, externally or even both. The internal attacks are no doubts the most damaging attacks as a

bank's personnel have authorized access to critical computer resources. The attacker with detailed knowledge relating to the bank's practices and procedures can easily gain a level of access. After that, he or she can potentially transfer money or other assets inappropriately (Milutinovic & Patricelli 2002, 88). Therefore it is of crucial significance to review and evaluate the security of internal networks. External attacks can be performed based on spoofing, eavesdropping, data alteration (Milutinovic & Patricelli 2002, 88). Thus online banking shall set the standards in terms authentication, privacy, data integrity, and non-repudiation.

Cryptography provides privacy through utilization of various types of cryptography algorithms.

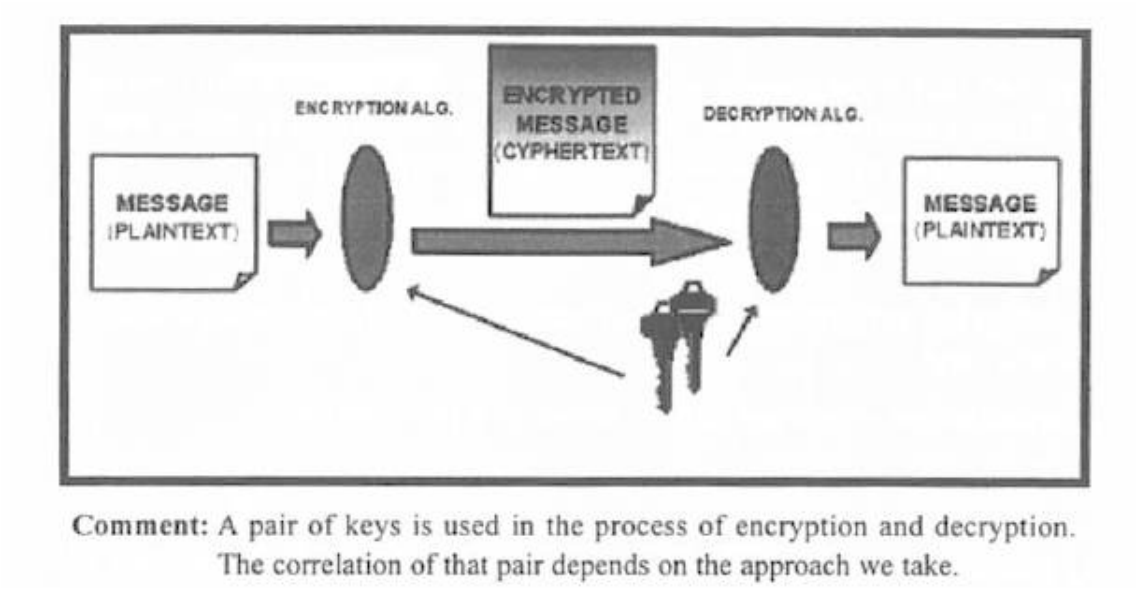

Figure 1: Simplified flowchart of the encrypted transmission (Milutinovic and Patricelli 2002)

The keys used in encryption/decryptions process are through three different approaches: symmetric, asymmetric, hybrid. In the symmetric approach, encryption and decryption use the same key for both sides. In asymmetric approach, the senders use the public key for encryption while the receiver uses the private key for decryption. The hybrid approach combines both fore mentioned methods. It uses symmetric approach to encrypt data and to pass the symmetric key through asymmetric approach. (Milutinovic & Patricelli 2002.)

Cryptography can provide privacy but may not necessarily prevent security from position in the open. Digital signatures set up three important electronic communication standards: origin authentication, data-integrity authentication, and non-repudiation (Online banking 2014). Origin authentication verifies whether the message is sent by a declared sender. Data-integrity authentication verifies whether the message is changed after it is sent. And non-repudiation prevents a denial of a previous act.

A false certification or no certification mechanism can result a “man-in-the-middle” attack. Thus the attacker can obtain knowledge over controlled data and gain access to data and resources. Milutinovic and Patricelli (2002, 92) explain that digital certificates generally offer the function of binding tightly from serveral attribute to the public key for example a name or an identity thus such in the middle of nowhere scenarios can be eliminated. Digital certificate is actually an electronic file which identifies communication entities in a uniquely way on the network (Milutinovic & Patricelli 2002, 92). IT associates the name of an entity with its public key. Digital certificates are issued and signed by the certification authority. Certification authority is trusted by everyone and is responsible for entity name and public key binding. Generally speaking, certification authority is designed for any entity with control of the authentication services and the management of certificates. Certification authority can be public (a bank), commercial, private firms, and personal. An example of a certificate can consist procedures as: key generation, matching the policy information, sending the public keys and information, verification of information, certificate creation, sending/posting the certificate, and loading of the certificate.

Nowadays, the most frequently used protocol in securing the website is secure sockets layer (SSL). It enables encryption and certification functionalities function in a TCP/IP environment. SSL can be seen as the basis for every e-Business trust infrastructure including online banking (Milutinovic & Patricelli 2002, 95).

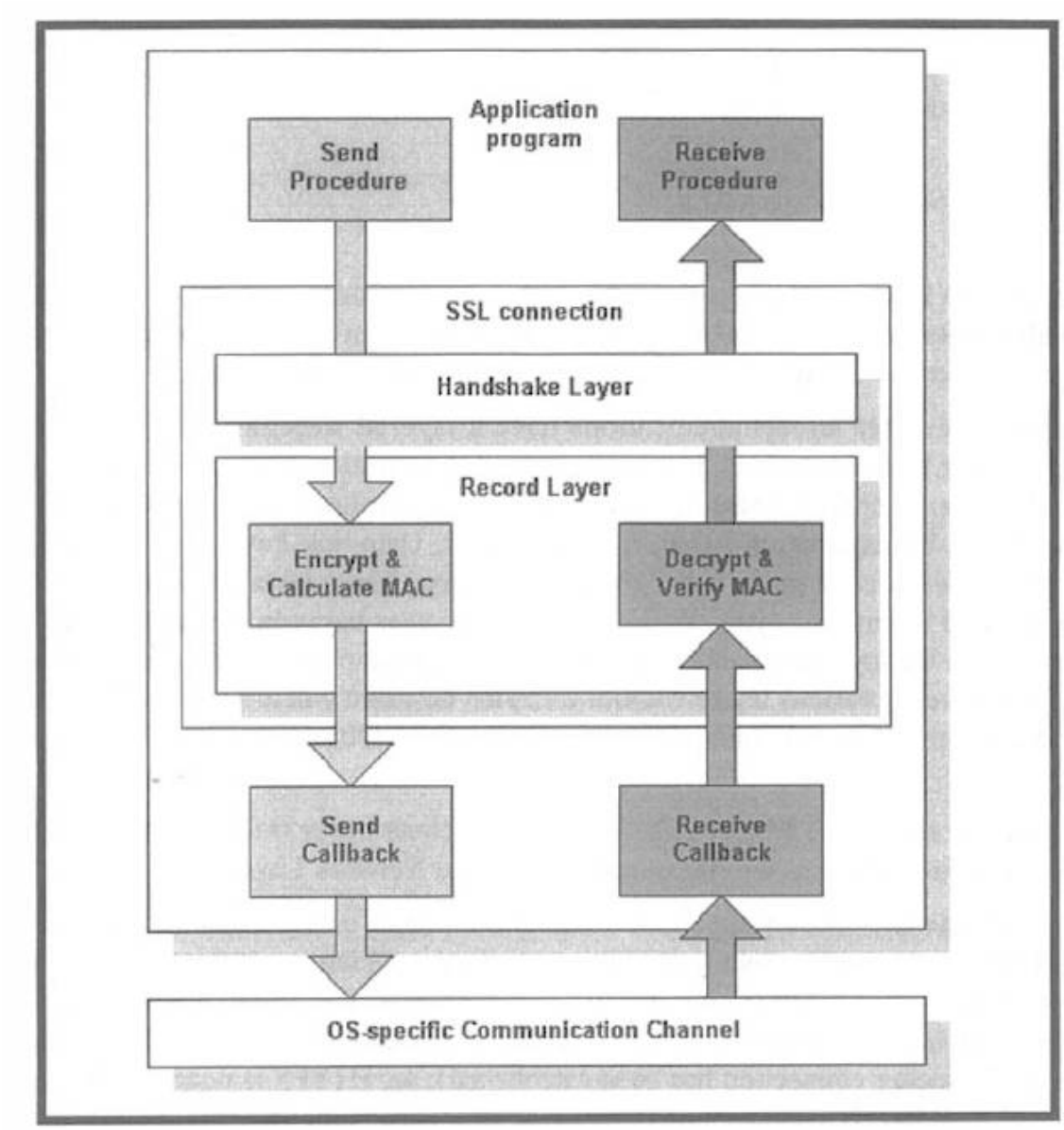

Figure 2: SSL connection and communication channel (Milutinovic and Patricelli 2002)

SSL protocol is composed of two layers which are the record layer and the handshake layer. SSL record layer provides connection security through encrypted data with symmetric cryptography. The message is also checked through keyed message authentication code for integrity assurance. A handshake occurs when SSL connection is required by a machine. The connection can be already open however for security reason it has to be hold on until the handshake is built successfully.

Aside from fore mentioned security standards, security shall also be secured from user's side. The user's sider of security is achieved through verification of digital certificates in the user's browser. When digital certificate arrives in the browser, the browser starts with checking whether the today's date is valid which means being within of the period of a certificate and

whether the certificated has been revoked. Then it checks if the issuing certification authorizes can be trusted by locating an issuer's distinguished name in the list of trusted certification authorities. If the certificate authority is a trusted one, the browser will check the issuing certification authority's public key against issuer's digital signature validity. Finally, it checks whether the domain name specified in the server's distinguish name matches the server's actual name. By completion all these procedures the verification is done. (Milutinovic & Patricelli 2002, 98-100.)

2.2.3 Characteristics

Comparing with traditional bank, online banking provides remote financial services for customers with the help of emerging information technology.

First of all, the main characteristic that distinguishes online banking and traditional bank is virtual property. Online banking relies on the rapid development of Internet technology to break through the traditional banking service mode which is face-to-face service in the counter. Online banking activities are conducted through the virtual digital platform that provides financial products and services to customers. In the online banking service, there is not specific person providing services for customers but the operating servers. The service and information from online banking cannot provided in paper format to customers, however all trading information will be stored and presented in online banking information system in the form of electronic data. Because of this characteristic, both retail and enterprise customers are offered with more convenient and efficient services. At the same time, the virtualization of online banking has brought great difficulty in terms of supervision, control, and legal issues. (Laforet & Li 2005.)

Secondly, information asymmetry is another main characteristic of online banking. Although the information asymmetry exists in most of the industries, the situation is worse in financial industry. Though the decentralized shareholders and creditors may sign and implement effective incentives contract, debt contracts will restrain manager from evaluation and supervision. Due to the information asymmetry that appears in online banking business of bank with virtualization, it will even lead to new asymmetric information problems. For example, in the process of trading in online banking, customers rely on the information published by bank so they have no much choice with financial products and services. At this time, if there is no legal constraint, the information published by bank only can rely on the publication of consciousness and marketing constraints. (Laforet & Li 2005.)

Thirdly, online banking has economic characteristic, which is derived from the fact that it drastically decreases trading and operating costs. Laforet & Li (2005) outline that comparing

with traditional bank, online banking do not require actual counter or a large number of personnel but the hardware, software and the related technical and managerial personnel. Furthermore, it is different from the traditional bank which possesses regional characteristic. Focusing on a unified global market, online banking not only exists in regional but also all over the world. As a result, online banking significantly reduces costs of bank operation management.

Fourthly, high risk is the typical characteristic of online banking. It includes two aspects: high risk in bank operation management and online transactions (Laforet & Li 2005). As a matter of fact, any business would undertake certain risk. However online banking may bear higher risk that different from other business. Worth mentioning, the high risk existed in online banking is inherent, infectious and global.

Lastly, online banking shares the characteristic of openness, which is a pivotal factor distinguishing itself from traditional bank (Laforet & Li 2005). To sum up, online banking breaks though the traditional way which is face-to-face mode with limited region. Online banking enables customers obtaining the financial products and services anytime as long as the Internet is connected to the needed equipment. In the meantime, the breakthrough of online banking in region brings challenges for its regulatory.

2.2.4 General risks

This sub-chapter presents the general risks including operational risk, network security risk, credit risk, transactional risk, reputational risk and legal risk, which could be potentially occurred in online banking field.

2.2.4.1 Operational risk

According to Zhao, Koenig-Lewis, Hanmer-Lloyd and Ward (2010), Security risk happens when there is inadequate access control allowing hackers attacking the bank system via network and leaking out confidential information. System design sometimes can also be unavoidable risky as being lack of implementation and maintenance regarding joint embodiment, dependence of external service providers. Customer misuse risk is appealed when the bank does not conduct adequate safety publicity and education on the prevention of the problem to the customer. The bank's internal organization and management of risk is associated when Internet banking has changed the traditional business model of the bank while the bank does not carry out internal organizational and management changes.

2.2.4.2 Network security risk

Due to the particularity of technological development, securing online banking system might have the network security risk with mainly two aspects. One can be the risk brought by the security certificate system failures. Given to the fact network is a naturally virtual, both sides that commit the transaction cannot ensure the genuine identity. It is therefore very difficult to build trust and sense of security. Another type of risks is caused by attacks from hackers and viruses. According to the latest statistics, over 40% hacker attacks were targeted on financial systems worldwide and severely jeopardized online banking operations. Securing the transaction safety, capital and account safety, and information safety has become the priority when developing online banking. At the moment, several banks have already taken actions to protect online banking security and have set standards and principles. However, potential risks are still existed due to the facts such as lack of strict management, backups against catastrophes, virus protections and etc. (Zhao et al. 2010).

2.2.4.3 Credit risk

All businesses operated by financial institutions are based on perfect and complete credits. Adverse selection and moral hazard will be inevitably occurred and impact the incomplete credit system which is more or less resulted by the asymmetric information flows in the financial operation progresses. The unique role online banking requires a higher level of completeness of credit system. As a matter of fact, credit system in China is not quite yet complete. It is actually imperfect and immature. Therefore many firms are not willingly to accept the electronically settlement and personal small amount transactions are more inclined with cash transaction. Such "conservative" financial habits greatly restrain the development of online banking. To sum up, building complete information protection mechanism, ensuring the adequacy and symmetry of information are the key to the success. (Zhao et al. 2010.)

2.2.4.4 Transactional risk

Transaction risk refers to cheats, mistakes, high-risk investment, and the investment bringing immediate or long-term financial loss (Zhao et al. 2010). Online banking is often accompanied with huge transaction risks, especially when the products are immature, with insufficient plan, implementation, and supervision.

2.2.4.5 Reputational risk

Reputational risk implies that the negative effects will be enlarged and spread when customers' requirements are not met and customers become unsatisfied. In general there are four

aspects resulting such risk. The first one is the technical defects of system. System errors or imperfect designs may lead to customer login failure or customer information loss. Such disturbing and unsettled issues may disappoint customers and result the loss of customer trust and loyalty. The second one is the severe system leak. When hackers attack or virus has been implanted into the banking system, severe system damage may be resulted such as data corruption, system disorders and etc. Aside from gigantic financial loss, large number of customers may be scared and leave the "problematic" bank. The third aspect is word-of-mouth. When the same or similar problem happens during the user experience, the customers may complain it to their friends or colleagues which results even larger customer loss. The fourth one is very similar to the third one. However it concerns bank reputation regarding the whole banking industry rather than one single bank. When a global bank has been revealed of reputational crisis regarding online banking or electronic transaction, customer will doubt the system security of other banks as well, and the trust crisis will be spread to the whole banking system and influence the stability of the banking industry.

2.2.4.6 Legal risk

Currently, online banking is at very beginning of development. It is still in the progress of constructing and improving with regards to a series of laws and regulations matching. Therefore, the existence of legal, regulatory loopholes and deficiencies will be inevitably. For example, the problem such as electronic funds transfer, the legal protection of credit relationship between banks and enterprises as well as the legitimacy of service and trading agreement should be further defined. Besides, China has no available specification and implementation of online banking standards yet, such as the core technology of online banking business, which includes the identification authentication of authority and independence, data encryption, commercial password products, communications security and the technical parameters. In other words, the legal environment of electronic commerce established in China is not mature yet, so banks will encounter and face various legal risks.

2.2.5 The current status

In recent years, the rapid development of Internet offers a solid foundation of hardware facilities and the huge user base for the rise of online banking. The online transaction and payment, which is based on online banking, is also the key point of implementing e-commerce. At the same time, the rapid development of e-commerce further promotes the popularization and application of online banking.

Since 1995, the first safe American online banking has been founded. The online banking business in developed countries flourished ever since. Citibank, Bank of America, JPMorgan

Chase Bank, Deutsche Bank, Royal Bank of Canada, Hong Kong and Shanghai Banking Corporation (HSBC) and other international financial conglomerates thrived in online banking market. Within a decade, as a new banking model, online banking has been widespread all over the world whereas its unprecedented effects influenced on the traditional banking and even entire financial industry. (Chinese E-banking Evaluation Report 2013.)

Online banking is booming in China as well. Since 1998, the "all in one net" online banking service of China Merchants Bank (CMB) has been officially launched and till now has 15 years online banking history in China. Nowadays, most of the major banks in China consider online banking business as the most prominent part to their business. In 2010, the "Super Internet Bank" has been launched and has connected each port of online banking from various commercial banks. Currently, more than 30% people in the urban areas have used personal online banking which indicates the online banking industry in China shall develop continually and dramatically. By the end of 2011, the amount of personal online transaction in national bank mounted RMB369 million while the total transaction amount of online banking business reached RMB695 trillion. (IResearch 2013.)

3 Research methodology

In this chapter, the author will argue for the understanding of selection of research approach and study design. Then reasoning of data collection, analysis will be presented.

3.1 Research approach

In all academic research, the description of research approach within one study is the first stage. Qualitative method, quantitative method, and the hybrid method are most commonly used research methods. Qualitative method is to definite an object or a phenomenon and then investigate the reason why the phenomenon forms and how it forms. Quantitative method is to analysis an object or a phenomenon in collecting a certain amount of resources and then compare them regarding the changes in numbers or quantitative relation to obtain the result. Hybrid method combines both qualitative and quantitative methods. Generally, the characteristics among this approaches are similar while the data collection and data analysis are different.

3.1.1 Qualitative method

Mark (2009) argues that a quantitative study is majorly adopted when data collection method or data analysis process are numerical data. Meanwhile, utilizing qualitative study is usually when data collection method or data analysis process deal with non-numerical data.

Holme and Solvang (1991) argue that the quantitative approach requires researchers to be positioned outside of the case and to gather research data in a rather objective way. Quantitative research shall determine the level of certain phenomenon through form of the numbers (Zikmund 2000).

The qualitative approach allows the researchers to have a deeper understanding of a certain problem (Zikmund 2000). The qualitative method is used to gather the information with a great degree of freedom and therefore are generally adopted when several problems or specific question within research need to deal with. To conduct a qualitative study, conversation, surveys, and interviews are frequently used.

The quantitative approach enables the carried out research results in a more objective manner as information is gathered and conclusion is drawn in a scientific and systematic way (Saunders 2009). The purpose of this study is to explore the online banking security issues of the ABC. It is a study with an in-depth understands rather than hypothesis-based or statistically based. Thus qualitative method will be applied in this study.

3.1.2 Deductive study

When researchers develop and build theories in scientific level, the deductive approach and the inductive approach are the two main approaches. As Mark (2009) points out, a deductive approach is used as to develop a theory with hypothesis/hypotheses and to design a research strategy testing the hypothesis/hypotheses. On the other hand, inductive approach is used when data is collected beforehand, and will developed into theory as the result of data analysis. The deductive approach starts with a theory base and formulation of hypothesis. Then the data will be collected to test and validate for the hypothesis (Saunders et al., 2003). Inductive approach could be alternative when the researcher would conduct a research. The inductive approach can be regarded as the one of the every first step in scientific methods where researchers can observe facts and generate theory through such approach (Ghauri and Gronhaug 2005).

In this study, in order to examine the theories and predictions which were already existing, the author selected the deductive approach for the research. As it lacked of sufficient study previously discussing online banking of the ABC in terms of its online activities security issues.

3.2 Research design

Mostly used research methods' literature appears to be the threefold concerning the classification of research purpose are exploratory study, descriptive study and explanatory study(Robson 2002, 59). Robson stated that an exploratory study is an effective approach to figure out that to define the phenomena, to find the new outcome and to evaluate it based on innovational mind (2002, 59). Due to the new direction is identified by him, hypotheses rather than examines or describes the existing one, it is the main difference compared with other approaches. It is generally used by researchers for clarification of the understanding of certain phenomenon or problem.

Robson argues that describing a specific person, occurrence or circumstance is the purpose of descriptive research (2002, 59). The researchers initially indicate the collecting data, then draw the conclusions and synthesize ideas in such study.

Studies establishing causal relationships between variables are usually termed as explanatory research. Indicating one phenomenon and giving answer to the "how" questions is what does explanatory research do (Ruane 2006). It can be referred to as cause-and-effect analyses aiming at identifying and explaining certain occurrences. The studying of one phenomenon is emphasized by explanatory research as to define the variables relationships in depth (Saunders et al., 2009).

Therefore, the author concludes that as in accordance with Robson (2002), an explorative approach had been analyzed and utilized all over this study. The approach is to gain new insights from the findings. This study targets at exploring the online banking security issues of the ABC in order with the above procedure.

3.3 Case study strategy

Experiment, survey, case study, action research, grounded theory, ethnography, archival are the five widely used feasible research strategies (Mark 2009). Mark states that survey is the most generally utilized strategy regarding deductive approach, it also gives answers about the investigator's identify, investigating questions, the quantity of investigation (2009, 144). While he further explains that archival research strategies are used when the answer to the research question will be longitudinal rather than cross-sectional. The answer can be either exploratory, descriptive or explanatory (2009, 150).

According to Yin (2003), there are four kinds of case study strategy including single case, multiple case, holistic case, and embedded case. Mark (2009) describes that the strategy about a single case is used to present a unique, critical, or an extreme case. While multiple case study strategy is applied to conduct cross case analysis and to compare relationships among

cases. The study in this thesis is to explore the specific risk factors of online banking which is a specific case, therefore a single case strategy has been applied in this study.

3.4 Collection of data

In general, data collected can be divided into primary data and secondary data. Primary data is the data collected by the person who conducts the study, secondary data is the data collected by others for other research purpose.

3.4.1 Primary data

Primary data is collected specifically for the purpose as to address to a specific research topic. Primary data is therefore more related to the research topic other than secondary data. Usually primary data is collected by interviews and questionnaires. Primary data allows researcher to set and adjust data collection manner in accordance with the research topic requirements. The initial collected data has adequate connection to the research topic.

As this study aims at exploring the online banking security issues of the ABC, primary data will be needed as to assist the author to further and deeply understand the related research factors.

Interviews establish an effective and efficient interaction connection between the interviewee and the researchers (Ghauri and Gronhaug 2005). Wrenn (2002) concludes that interviews can be conducted in various ways: personal interviews, mail interviews, and phone interviews.

Generally speaking, there are three types of interviews which are structured interview, unstructured interview and semi-structured interviews (Ghauri & Gronhaug, 2005). Maintaining a brief and clear logic Structured interviews are the function of structured interviews. And questions in interview are standardly set to a specifically target respondents. The major merit of structured interview is allowing researchers have right to assess all respondents with an unbiased manner. However open questions cannot be put up during such interviews.

Refer to unstructured interviews, it provides researchers great freedom for making questions or further discussion. And meanwhile unstructured interview has a certain requirement of the interviewers' ability in order to guide the interviewees to answer questions for analysis. This kind of interviews are more flexible, in-depth, but can as well be either highly topic-related or highly topic-unrelated.

Turn to semi-structured interview, it is the interview differs from other interviews as it is an approach used by interviewers to gain information or knowledge. The interview result is mainly information and knowledge with regards to the related research topic rather than pure data.

Since the research is aiming at having an in-depth understanding regarding online banking security issues of the ABC, it is significant that the data collected being clear and comprehensive. The author decided to conduct a semi-structured interview with the manager of online banking IT department who is in charge of building IT infrastructure and safety issues.

3.4.2 Secondary data

According to Mark (2009), the data collected by others for some other purpose is known as secondary data. Ghauri and Gronhaug argue that secondary data is an important source as to assist researchers gain better understanding and views of their research problem (2005). Some research questions can merely be answered through analysis of such data when no further primary data is gathered.

In this research, the secondary data is collected and consisted of the sources which are mainly from external and internal. Literature which is existing, materials and documents which are published regarding this research subject are composed of the external sources. And webpages, files and reports from the internal of ABC are consist of the internal sources.

3.5 Data analysis

In this research, the explanation building technique is adopted. In this study, the ABC had been chosen to conduct a single case study. The data was collected through interviews, webpages, internal documents and related literature. The author analyzed data through two aspects which were strategic and technological. Then the comparison between data at hand and frame of references was made.

3.6 Validity and reliability

Paying more attention for the research design which mainly including reliability and validity is providing the possibility of decreasing the mistakes in data collection and data analysis (Saunders et al., 2009).

As Saunders et al., point out that the great consistency of findings yielded through data collection and data analysis means reliability (2009, 156). The result from semi-structured inter-

view in a qualitative research may not be either enough objective or accurate. It is very hard to make sure the reliability of qualitative data. It is based on the understandings of the author and the interviewees. In order to make sure that reliability of the interview in this study, questions have been sent to the building IT department manager Xiaoxin Yuan before the actual interview. Thus enough time would be left for the manager to prepare for the answers.

As Saunders et al., explain that the accuracy and adequacy of the findings towards related research are ensured in order to achieve validity (2009, 157). The research study is to present and analysis information regarding online banking security, therefore the author select to interview Xiaoxin Yuan and the author was positive that the interviewee was capable of answering the topic related questions as to enhance the validity level. Furthermore, the interviewee received the interview questions several days ahead of the interview so that he has sufficient time to understand the background and context of the interview. According to above, the author believed the interview is trustful with high quality.

4 Empirical case

In this chapter, the case finding will be present. The author will firstly introduce the background information of ABC, then continue with presentation of interview result as well as related information.

4.1 Case: online banking in the ABC

This sub-chapter demonstrates the case of online banking in the ABC which sets a good example for other Chinese banks concerning online banking security protection. The system functions, characteristics, system mechanism for corporate online banking and personal online banking as well as the online banking payment system guarantying solutions are introduced separately. It also elaborates features and concerns of the whole development of ABC's online banking system and the corresponding counter strategy in the end of sub-chapter.

4.1.1 System functions

User management function includes creation of new users and inquiry of log. USB-KEY management function consists of installation and deletion of USB-KEY software package. Digital certificate management includes certificate application, download, update, inquiry, backup and recovery. Service function contains account, accounting inquiry service, transfer and remittance, report of loss and change of password, self-loaning, online payment and foreign currency buying and selling and etc.

4.1.2 Characteristics

There are five characteristics of ABC's online banking system described in this sub-chapter: digital certificate, perfect security mechanism, value-added service function, free to set the limitation of payment and updating and optimizing USB-KEY. These characteristics are provided for having a good understanding for ABC's online banking system and functionality.

4.1.2.1 Digital certificate

Definition

Digital certificate is identification for customer doing online trading and business activities. Based on the certificate, customer can encrypt data and signature. The online banking transaction data, which be processed by digital certificate, cannot be modified. The uniqueness and nonrepudiation of that can prevent others pretend certificate holders to do online trading, and then safeguard the legitimate rights and interests for users and bank meanwhile reduce and avoid the economic and legal disputes.

Functions

Identification of both sides of transaction will be confirmed. Generally speaking, online banking server will confirm the identification of certificate's owner and the client will also test the legality of website through website certificate. Information shall be of completeness and confidentiality.

Storage carrier

Digital certificate can be stored in the IE browser, IC cards, USB key and etc. The digital certificate (including the private key) in the IE browser can be derived from the brower and backed up. As the private key can be copied, it can be again derived in the browser. So it must be carefully protected. However, private key stored in IC cards or USB keys cannot be copied, therefore IC cards and USB keys reach high security level.

4.1.2.2 Perfect security mechanism

The mechanism for transaction authentication is complete and meets the international standard. Closed communication protocol developed by the ABC has been adopted for the use of Network communication and prevents the communication to be hijacked.

4.1.2.3 Value-added service function

Under the safe and complete online banking mechanism, personal remittance, transfer such functions with high demand of safety is added into system. The system also includes fund investment, insurance, bonds, and financial services to improve individual online banking experience.

4.1.2.4 Free to set the limitation of payment

Client can choose whether to cancel the limitation of maximum online payment. On one hand, client can only the safety mechanism in a more customized way and on the other hand, it becomes more convenient for customer when they want to pay for a large amount.

4.1.2.5 Updating and optimizing USB-KEY

USB-KEY has been through evolution from generation 1 to generation 2. Generation 2 USB-KEY is designed based on the concept of interaction between machine and people. Compared to the widely used normal USB-KEY, the hardware such as buttons and screen and the configuration has been updated to better defend the attacks from hackers.

4.1.3 The security mechanisms for corporate online banking

The ABC has established a very secure online transaction platform in corporate service. The whole transaction process is protected with data-encrypted precautions and is constructed as a safe bridge connecting clients and the bank. Both client's and bank's digital certificate will be checked when a transaction is about to begin. If the certificates work on both sides, which identities are all confirmed, then the client will use digital signature to authorize the digital signature. Then the transition will be completed. The online banking of the Bank has passed through the authorized third party assessing agency in China and therefore is of reliability.

4.1.3.1 Transfer security

All data between client server and the bank server has been double encrypted. The first level encryption applies SSL protocol to prevent data from decrypting, deterring or revoking. The second level encryption is encrypted by private protocol, which is of confidentiality and safety.

4.1.3.2 Virus protection

Under the reliable data transmitting mechanism, data between client server and the bank server is conducted with a certain types of format rather than applications. Client server

strictly examines whether the formats are appropriate therefore it ensures no virus shall invade the online banking system.

4.1.3.3 Strict authorization management

In terms of paying salary or any other sensitive fund transferring business, online banking system has applied strict principles and regulations with differentiated levels of authorization and access control.

4.1.4 The security mechanism for personal online banking

Online banking services include managing personal deposit, online payment, online stock service and etc.

4.1.4.1 Technologic means

The following is a detail demonstration of the ABC login procedures. The first one is the production of certificate and load in with encryption

1. Login to the ABC website www.95599.cn, then click on certificate guide as can be seen in the red marked in the picture (all the following pictures come from this website)

Figure 3: Screenshot of ABC Website Online Banking Login. (ABC website 2014)

2. Click browser certificate

Figure 4: Screenshot of ABC Website Online Banking browser certificate. (ABC website 2014)

3. Click download browser certificate

Figure 5: Screenshot of ABC Website Online Banking downloading browser certificate. (ABC website 2014)

4. Enter the reference number and authorization code from the envelop you get when you apply for online banking service

Figure 6: Screenshot of ABC Website Online Banking entering code. (ABC website 2014)

5. Click next step when a window pops up declaring the media is browser certificate

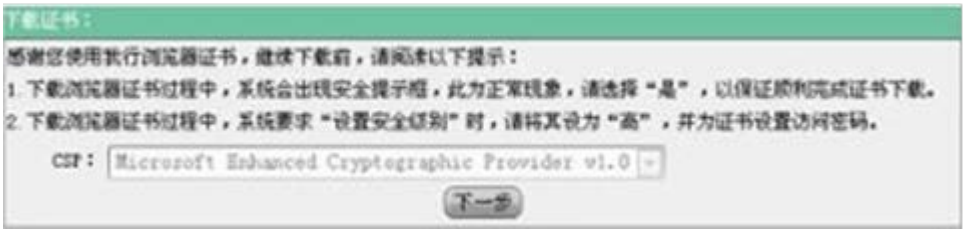

Figure 7: Screenshot of ABC Website Online Banking CSP window. (ABC website 2014)

6. When CSP is provide, system will generate a key randomly and a new cross window will pop up where customer can set security level of the downloaded certificate and category of the passcode and the passcode.

Figure 8: Screenshot of ABC Website Online Banking passcode. (ABC website 2014)

7. Click done, after a while the new client certificate will be generated.

Figure 9: Screenshot of ABC Website Online Banking New certificate window. (ABC website 2014)

The following procedure is to derive the encrypted certificate.

1. Open browser and find tool, select Internet option, select content, select certificate.

Figure 10: Screenshot of ABC Website Online Banking Opening browser window. (ABC website 2014)

2. Open the certificate management window

Figure 11: Screenshot of ABC Website Online Banking opening certificate management window. (ABC website 2014)

3. Select for the certificate and click derive

Figure 12: Screenshot of ABC Website Online Banking Selecting and deriving certificate window. (ABC website 2014)

4. Click next, the system will inquire whether derive the private key, select the key and click next

Figure 13: Screenshot of ABC Website Online Banking System inquire window. (ABC website 2014)

5. Choose the file format as private information exchange and select use strengthen protection and click next.

Figure 14: Screenshot of ABC Website Online Banking Choosing file window. (ABC website 2014)

6. System requests entering passcode for backup files. The passcode will be used the recovery of certificate thus must be remembered firmly.

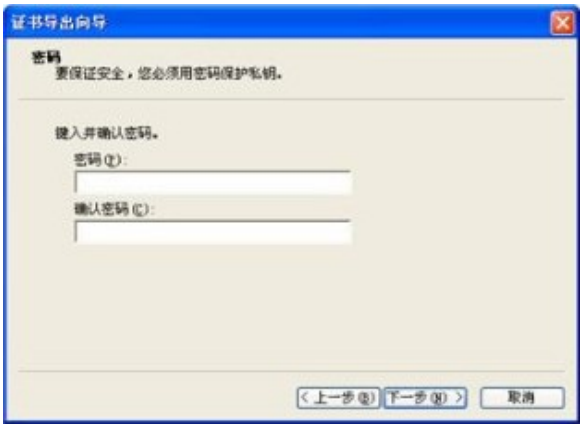

Figure 15: Screenshot of ABC Website Online Banking System requests window. (ABC website 2014)

7. Save the document

Figure 16: Screenshot of ABC Website Online Banking Saving document window. (ABC website 2014)

4.1.4.2 Business security monitoring solution

There are various restrictions to ensure online transaction safety especially when it comes to the self-online banking transferring, online payment and etc. There are limitations for the maximum transfer amount, the maximum transfer frequency and detailed information for tracking the flow of transfer.

4.1.5 Online banking payment system guarantee solutions

The online banking payment system plays a pivotal role in the whole network system. In order to understand how individual online transaction activities can be conducted in a safely manner, this sub-chapter shall present five guarantee solutions from account and password, phishing site, anti-virus software, firewalls and to other bank services aspect to offer the general announcements on using online banking payment.

4.1.5.1 Protecting own account and password

Bank account and password are absolutely private information which shall not be leaked out. One shall change password in a certain period of time.

4.1.5.2 Using separated banking password

Bank password shall be different from the passwords with other uses. The bank also suggest customer using different passwords for inquiry, withdraw, and online payment.

4.1.5.3 Beware of phishing site

The bank recommend customers to start any online banking activities with its official website other than any other websites especially given by strangers.

4.1.5.4 The use of anti-virus software and firewalls

Firewall is very protective and cuts the connection between attackers with the targeted computer. The bank suggest customer setting the firewall protection level to the highest when conducting any transaction activities as so to avoid online bank robbery.

4.1.5.5 Utilize the value-added services from bank

The ABC provides SMS and email whenever a transaction has been conducted. Therefore customers can take full advantage of such close service to keep their financial states updated. As long as any inappropriate transaction occurs, customer can notice it in the first place and take actions to get back the lost fund and prevent further loss.

4.1.6 Features and concerns

Based on the current Chinese financial system, online banking network infrastructures and the related legal framework, different features and problems have been formulated. Online banking is developed through the informatization and cyberization of traditional banking. The business range and scope of traditional banking has been extended and enhanced by online banking. At the moment, individual client's education level and information technology knowing lie in a higher level comparing the understanding and appliance of information technology from the enterprises. The major online banking risks are mainly resulted from the lack of legal regulations and incompletely developed IT infrastructure. The external supervising system is lagged and the current law and regulation system mismatch. Cyber fundamental infrastructures shall be strengthened and the network environment needs to be improved.

4.1.7 Counter strategy

The ABC aims at strengthening its business system by providing initial activities with innovation, completing and improving business range and scope, service versatility. Online banking system shall be presented as a "financial supermarket" with one-stop shopping experience. Considering the operational strategy, The ABC determines combining both traditional and cyber banking mechanism, endeavoring to provide its customer with a variety of choices. Regarding the operational concept, The ABC aims at realizing the transition from product-oriented focus to customer-oriented focus. Providing services which are tailored by customer demands and needs. Last but not least, The ABC furthers its cooperating with other major financial institutes to become an important economic gateway.

5 Analysis

In this chapter, the analysis of the case finding will be presented. The analysis will be generated based on the theories from the theoretical background part.

5.1 Risks and concerns

As we can see from the case, different features and problems have been formulated. It is influenced by the current Chinese financial system, online banking network infrastructures and the related legal framework. As online banking is the extension of traditional banking, the business range and scope of traditional banking has been extended and enhanced by online banking. However. The major online banking risks are mainly resulted from the lack of legal regulations and incompletely developed IT infrastructure. The external supervising system is lagged and the current law and regulation system mismatch. Moreover, network fundamental infrastructures need to be strengthened and the network environment requires improvement.

5.2 Precautions

This sub-chapter describes that the precautions for online banking risks from two aspects: educational and technological.

5.2.1 Educational aspect

From the educational aspect, the bank recommend client to treat client password like a toothbrush: change it frequently, and do not ever share. Strong passwords are used as the first line of defense in online banking activities. The ABC suggests its client to start alert when receiving email or SMS from a stranger who is pretending to be your friends or relatives and to avoid clicking on insecure websites.

When client create an online account at The ABC website to access his or her actual bank account, client will need to supply an email address, username and password. The bank suggest the client using the email address to create a new email account to use only for financial matters other than the use of general correspondence, and to keep this email address private. It keeps the information of confidentiality.

The ABC can also provide client alert by sending email confirmations of online transactions. This will provide client with an early warning of any fraudulent activity.

Malware on client's computer can put the bank account at risk. The ABC offers a wide variety of suggestions to help client be vigilant against the threat of malware. The ABC informs client to install anti-malware software and regularly run scans of the computer and not to click on links in emails clients don't trust. Also the ABC educates clients not to visit suspicious websites, and to use website trustworthiness checkers to examine uncertain websites before visiting.

5.2.2 Technological procedures

For the technologies aspect, the ABC provides trustworthy digital certificates and upgraded USB-KEY to keep online banking activities safe. HTTPS and SSL authentication technologies are adopted. Clients will have to download certificate packages from the ABC official website to login and further their financial activities.

As we can see from the case, the ABC establish "dual control" over clients account as adopting USB-KEY. Once this safeguard is in place, two individuals from the client server will need to log on and authorize any transaction. With dual control in place, the hacker will have to breach two computer accounts in order to commit a fraudulent transaction.

Under the reliable data transmitting mechanism, data between client server and the bank server is conducted with a certain types of format rather than applications. Thus the data is protected strictly and examined in terms of the formats therefore it ensures no virus shall invade the online banking system.

When it comes to the salary or any other sensitive fund transferring business, the ABC has applied strict principles and regulations with differentiated levels of authorization and access control. It is in accordance with integrity and providing authentication to access.

6 Conclusion

The final chapter here is the conclusion of the thesis shall be presented. And some advises and suggestions will be given to the researchers to continue the study within this area and to conduct future researches.

As the purpose of this paper was to explore risks factors of online banking of in the context of Chinese banking industry. Furthermore the author has sought to identify precaution techniques used by the bank from both technological and educational viewpoints. The author has chosen one of the largest Chinese bank, ABC to conduct the research. ABC as a leading bank in China with sufficient experience and appropriate precautions against online risks, has world class standard and can represent the highest level of online services provided in the banking industry. A qualitative research method and case study strategy were selected as the research method with a deductive approach in order to examine the protection methods used by the ABC against different network security standards. The result and outcomes here is research questions are addressed below and related topic implications in the context of Chinese online banking industry are followed.

6.1 Results and outcomes

By analyzing the empirical findings from the interviews, company reports and Internet sources regarding the Chinese leading bank ABC, the author would like to draw the conclusion of this thesis. Firstly, the results of case study are presented here.

RQ1. What are the factors that bring risks to online banking security of the ABC?

In this study, the ABC reflects the commonly faced online banking security risk factors which were poor policy and legislation, the economic system at the moment, and the immature IT infrastructure. The external supervising system is falling behind the current online business environment while the laws and regulations system mismatch the current online business status. Therefore the external supervising system as well as laws and regulations system cannot fulfill the tasks and requirements regarding online security issues and become ineffective. Worth mentioning, though ABC provides its clients with online transaction platform based on a relatively complete and secure IT infrastructure, the whole IT environment is immature and concludes deficiencies. On one hand, users may possess inadequate IT knowledge, online business experience and etc., especially when the users are from the enterprise online banking as individual client's education level and IT knowledge lie in a higher level comparing to the understanding and applicant of IT from the enterprises. Besides, the IT environment is contaminated with hackers, virus, and frauds and so on which unsettle both banks and users to an extreme extent.

RQ2. What protection methods are adopted by the ABC in order to reduce the risks?

The precaution techniques are adopted from two different aspects which are educational aspect and technological aspect. From the educational aspect, the bank educates its clients to change password frequently, to stay alert when receiving email or SMS from strangers who pretends to be friends or relatives and not to click on insecure websites. The ABC offers a wide variety of suggestions to help client be vigilant against the threat of malware. The ABC informs client to in-stall anti-malware software and regularly run scans of the computer and not to click on links in emails clients don't trust. Also the ABC educates clients not to visit suspicious websites, and to use website trustworthiness checkers to examine uncertain websites before visiting. The bank suggest the client using the email address to create a new email account to use only for financial matters other than the use of general correspondence, and to keep this email address private. It keeps the information of confidentiality. From the technologies aspect, the ABC provides trustworthy digital certificates and upgraded USB-KEY to keep online banking activities safe. HTTPS and SSL authentication technologies are adopted. Once this safeguard is in place, two individuals from the client server will need to log on

and authorize any transaction. With dual control in place, the hacker will have to breach two computer accounts in order to commit a fraudulent transaction. Under the reliable data transmitting mechanism, data between client server and the bank server is conducted with a certain types of format rather than applications.

6.2 Implications and Future Research

The author would suggest that future research could put more effort on comparison between large banks like the ABC with relatively small banks regarding online bank security issues. The author would suggest that researchers could combine an inductive research with a quantitative research methods which analyzes the risk factors in a technical way rather theoretical way as this study. Worth mentioning, as this study is concentrated in segmentation of online banking, the authors suggest that the studies in other new segmentations would be of interests and shade the light upon relevant online activities security issues.

References

Agricultural Bank of China. 2014. Company Overview. Accessed 15 April 2014. http://www.abchina.com/en/about-us/about-abc/Overview/

Ghauri, P. & Gronhaug, K. 2005. Research Methods in Business Studies: A Practical Guide. 3rd ed. London: Prentice Hall.

Hakim, C. 2000. Research Design: Successful Designs for Social and Economic Re-search. London: Routledge.

Holme, I. & Solvang, B. 1991. Forskningsmetodik. Lund: Studentlitteratur.

IResearch. 2013. China Online Banking Research Report 2012-2013.

Junchi, H & Haokun, C. 2012. Key Dimensions of Customer Value Influencing CRM Performance. BBA. Business Information Technology. Jönköping University.

Krawerk, N. 2006. Introduction to Network Security. Boston: Course Technology/ Cengage Learning. Book from ebrary. Accessed 27 April 2014. http://site.ebrary.com.nelli.laurea.fi/lib/laurea/docDetail.action?docID=10228225&p00=introduction%20network

Laforet, S. & Li, X. 2005. Consumers' attitudes towards online and mobile banking in China. International Journal of Bank Marketing. 23(5). 362-377.

Network security. 2014. Last modified 1 May. Accessed 2 May 2014. http://en.wikipedia.org/wiki/Network_security

Online banking. 2014. Last modified 10 April. Accessed 27 April 2014. http://en.wikipedia.org/wiki/Online_banking

Online recruiting: what works, what doesn't. 2000. HR Focus. 3. 11-13.

Reichheld, F.F., & Schefter, P. 2000. E-loyalty: your secret weapon on the Web. Harvard Business Review, July-August, 105-113.

Research Methodology: An Introduction. http://www.newagepublishers.com/samplechapter/000896.pdf

Robson, C. 2002. Real World Research. 1st Edition. Oxford, UK: Blackwell Publishers.

Yin, R. 1994. Case study research: design and methods. 1st ed. Thousand Oaks: Sage Publications.

Yin, R. 2003. Applications of case study research. 1st ed. Thousand Oaks: Sage Publications.

Saunders, M., Lewis, P. & Thornhill, A. 2009. Research Methods for Business Students. 1th ed. New York: Prentice Hall.

Milutinović, V. & Patricelli, F. 2002. E-business and E-challenges. Amsterdam: IOS Press. Book from ebrary. Access 27 April 2014.
http://site.ebrary.com.nelli.laurea.fi/lib/laurea/docDetail.action?docID=10116453&p00=e-business

Zhao, A. L. & Koenig-Lewis, N. & Hanmer-Lloyd, S. & Ward, P. 2010. Adoption of internet banking services in China: is it all about trust?. International Journal of Bank Marketing. 28(1). 7-26.

Figures

Tables

Appendixes

Appendix 1:

1. What is online banking security?

2. Are you satisfied with the online banking security of Agricultural Bank of China by now?

3. What are the factors do you consider as to the barrier to the safety of online banking?

4. What protection procedures are provided by the Bank to enhance security level?

5. (If the manager mentioned the detail technology) can you elaborate more about how this technology functions?

6. Ask the same questions for other technologies.

7. Are these technologies of the international standard or are they the latest?

8. Do you educated or provide other help to your client thus improving online banking security?