STUDY ON THE INFORMATION SECURITY SYSTEM FOR BANK IN CHINA

Xichen Jiang, Zhenji Zhang
Institute of Economics and Management, Beijing Jiaotong University, Jiaotong University East Street, Beijing, China

Feng Cao
Institute of Economics and Management, Beijing Jiaotong University, Jiaotong University East Street, Beijing, China

Keywords: Bank, Information security, Information technology, Security system, Management.

Abstract: During the wide use of the new network technology in finance, the electronic finance, commercial services on the net, and the cash payment system bring convenience to us, at the same time, it also brings lot of hidden dangerous and financial risk. Now this paper will construct a security system for the information system in bank based on contemporaneous theory of information safety and using the combination of information technology and the methods of management.

1 INTRODUCTION

The usage of information technology in council, commerce and finance brings out big change of people's life style. We are enjoying the big transform of network technology, however, at the same time; we have to face the problems coming from the data and information attack. The safety threaten of the information system are becoming more and more serious. Lots of system holes are used for bad things. All of these can bring hard burden to the information system. What is worse, it will leak out the personal private information, commerce secret and country secret. It will cause break off of the bank operation system and cause lots of dignify. Nowadays, the data are becoming more and more concentrate, the problem of safety are becoming more and more stand out.

With the high pace of social development, high-tech is continuously applied to all aspects of our life, particularly the financial sector such as processing information transfer. For example, currently e-commerce, online banking and electronic remittance processing business are widely used in our banks. To some extent, the bank's computer data takes place of money as a general equivalent, the transfer of information using computer network has taken place of the physical exchange of notes. This will be the future of the financial industry; will greatly change the traditional social life, production patterns and social structures. Computer network spread rapidly in the banking industry, while providing convenience. However, how to ensure the security of bank computer network reliability is the problem.

While the bank's dependence on the information technology staffs is becoming more and more, the risk also becomes very prominent. This requires banks to strengthen their own vulnerability detection. However, weak awareness of security is the universal problem in China's banks. Therefore, how to ensure the information network system for banking services becomes particularly important.

2 PERTINENT KNOWLEDGE

2.1 The Concept of Information Security

Information security is to protect the secrecy, integrality, usability, controllable and undeniable of information, apply service and information facility. It consists of information environment, information network, information application and so on.

As searching correlative literature, we can find that the information development in our county's bank has been in the stage of operation system

Jiang X., Zhang Z. and Cao F..
STUDY ON THE INFORMATION SECURITY SYSTEM FOR BANK IN CHINA.
DOI: 10.5220/0003477201900195
In *Proceedings of the 13th International Conference on Enterprise Information Systems* (ICEIS-2011), pages 190-195
ISBN: 978-989-8425-55-3

conformity, concentrate of data. During the development of information technology, there are more and more threaten for information security. Their methods are changing all the time and now information security has been staring us in the face.

2.2 Status of Bank Information Security

Now the methods taken for information system security in China include the following:

(1) In the security for storage of database, the operation system encrypt the key field and come into field storage in order to ensure the validity of the data changing and keep from nonlicet data changing.

(2) Control accessing purview, foreground application and operation system set different purview for users in different levels when the users are trying to connect the database.

(3) Use cryptographic check for all local transactions; through the designed program to shield the system.

(4) When the application process is running, use the way of signing to identify the operator, and according to the operator's permission to control the operator’s right. However, current application lacks safety design and support issues.

(5) Taking into network security issues, banks gradually using router and firewall products, these products have a relatively strong network security technology. But the products focus on local problem rather the whole safety problem.

(6) Operations department develop and implement a series of management systems and operating rules, many of which related to computer security issues, standardize the behavior of staff at all levels. However, the safety management tools drops behind.

2.3 Security Problems of Information Systems of China Banks

China's information technology is not mature, first of all, from the national scale, the system facilities is not perfect, whether it is the completeness of the information system facilities, or the breadth of its application, diversity, the banking system has big gap with the developed countries; Second, it is the lack of qualified personnel, especially lack of maintenance talents for bank information security. The core issue has the following points.

1. Network security technology exist biases. Many people believe that information security is network security or computer security, so we put pressure on the network making the network complex. We set various control cards on the information superhighway; however the result is less effective. The most important point to protect is information, we should be careful in the data collection, storage, operating and analyzing.

2. Pay attention to the tools investment rather than management investment. Investment in network security is not entirely safe products investment and tools investment, it should also include policies, operating procedures and emergency handling mechanism and other aspects of investment. The use of security products and tools should have appropriate environment of supporting process management.

3. Application software in bank is very weak. Bank's application software is the carrier of information. Safety and quality of software is very important including software development life cycle and project management system. Nowadays more and more holes in safety including technical and management come from the quality of the production of software.

4. Bank’s information and data management contains safety holes. Most of the applications of large banks are in the host application, the operating system is relatively closed, and the information storage is relatively safe. But the data and information have risk in management, these data include a variety of core business reports, customer relationship data, office functions, risk control information, etc., the information on the system transfer through an open IP network transmission, because the system's security holes, it is easily penetrated by virus, loss of management information is sometimes more dangerous than the loss of business data.

5. Disaster prevention is a priority. With the centralization of data, security risks are also concentrated, often a data controls more than one financial information processing, directly related to the network's normal business, whether it is software, host or network, it will have a huge negative impact on society. In addition a variety of disaster may lead to the data center does not work, or even the loss of financial information. How to design information security from the angle of disaster, how to balance the investment and information security is a problem that we must face.

Previous research shows that the current researches in this area are from two aspects: management and information technology. This is a further research of previous research done by these two aspects in order to get a secure system solution.

3 THE BANKING INFORMATION SECURITY ARCHITECTURE

3.1 Security Risks of Banking Business

Security risks faced by banks, include the physical layer, network and system layer, application layer, and security management.

(1) Physical layer security risk. It includes natural disasters, damage to the equipment room because of accidents; power outages, disruption in line system; the room and line electromagnetic leakage, resulting in leaks and other system information.

(2) Network and system level security risk. Risks are caused by unauthorized access, malicious attacks, viruses, invade, wiretapping and other security ; operating system and database security vulnerabilities, improperly security settings, and low security level; lack of file system protection and control of operations, applications exist back door. Virus threat to security of information systems is an important factor; the virus may cause information leakage, data destruction or loss, network congestion, and many other serious consequences.

(3) Application layer security risk. Key business is facing the risk of impersonation and unauthorized access; data may be stolen or unauthorized access, modify and delete processing while transmission, storage process. The information exchange and sharing between different banks or between banks and other sectors bring potential information security risks.

(4) Management of security risks. Security management is the most important part of security. When the security products are becoming more and more, the safety management of the product itself becomes more complex. Also, because of security management organizations, institutions and norms is not perfect, there is a potential risk management. Poor management brings more threaten to the information system.

3.2 Design of Safety System

According to the characteristics of banking and security requirements, in accordance with the "network isolation, Fenwick protection; identity authentication, authorization management ; layers of protection, security management, "the security policy should cover physical security, network security, system security protection, application security, security management, building a complete, integrated information security system. Security architecture of the logical structure is shown in Figure 1 below.

The final sentence of a caption must end with a period.

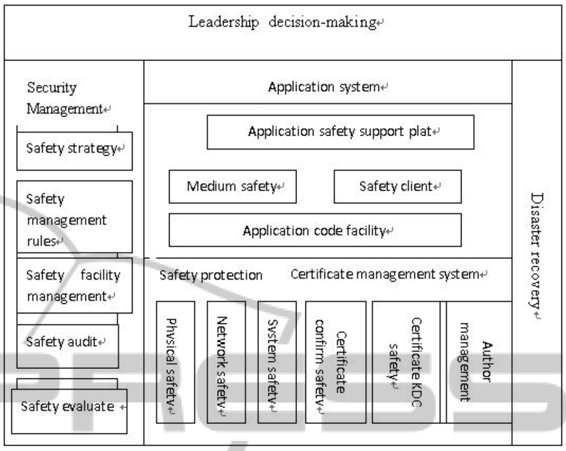

Figure 1: Security Architecture.

1. Leadership decision-making is in the top-level in the security system to guide the entire information security system's construction, implementation and coordination. Leadership decision-making system's guidance comes true through the safety management system. Safety management systems, security systems, certificate management systems and disaster recovery system not only have the level relations, but also interrelated, organic integration, showing safety from different angles. Application security support platform built on the security protection system and security infrastructure systems on the use of security services for applications and information system operation to provide security support for the protection, also accept the unified management of the safety management system.

2. Security Management

Banking network and information security management must keep the principle of the combination of management and technology. Comprehensive prevention, improve information systems security capabilities. Safety management system achieves commercial bank information network security management, security management platform specific implementation of the completion.

3. Construction of the Application System Platform

For the bank card systems, securities trading system, international settlement system, cash payment systems, treasury systems, debt bookkeeping system, foreign exchange transactions, open market operations and other financial products applications, these systems which have been running should be regulated, and as smooth as possible transfer to a unified platform. What is more, new online system should use unified platform. For the back-office applications of online banking, call centers, mobile banking channels and other services should concentrate to improve resource use efficiency, so that can form and maintenance the unified customer information.

4. Disaster Recovery

Bank's data centralization of data resources has the benefit of effectively integrated management and depth analysis to achieve communication between different applications and integration, so that can play the maximum value of the data. This can cause great impact on the operations of bank.. Meanwhile, the bank data centralization also brings new risks and challenges. To prevent the natural, human or technical reasons to cause the damage of system resources and system led to termination of service, we must establish the appropriate backup and fast disaster recovery mechanism. The main content of the disaster recovery plan covers the choice of the disaster backup center, construction and design of the recovery plan. We should further strengthen the banking center and backup data center's infrastructure. When we make system planning, design, feasibility studies, project implementation, testing, production preparation, switching stages before the data's concentrate, we should give full consideration to the safety of the system, and accept the competent authorities.

4 THE ESTABLISHMENT OF BANK INFORMATION SECURITY SYSTEM

The construction of bank information security is a combination of planning, management, technical, is a continuous process of dynamic development, which consists of safety management and safety technology. The two aspects are interdependent and mutually support each other; we cannot achieve the safety of the banking information network without either of them.

4.1 Establish Technology System to Ensure Banking Information Security

Computer network systems in the bank should use advanced network security technologies. Its technical means include access control, encryption and data integrity protection, identification and authentication, network anti-virus technology, firewall, backup and recovery, monitoring, audit tracking. The interaction between them in the order is shown below.

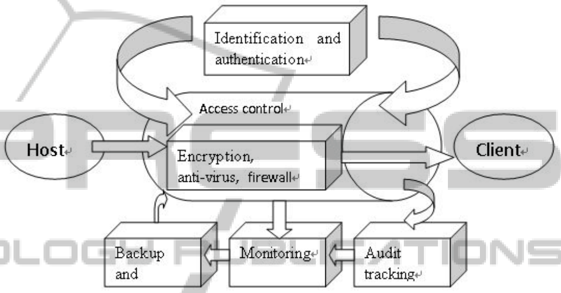
Identification and authentication
Access control
Host
Encryption, anti-virus, firewall
Client
Backup and
Monitoring
Audit tracking

Figure 2: Bank information security techniques.

(1) Access Control: In the application systems we create authorized operation or transaction definition table by setting up multi-level permission, provide different authority to operators in different level. After the server's verifying the identity of the user, it will determine the user's rights as his authority control information. The operator at all levels in the system can only be executed within the scope of its responsibilities.

(2) Data encryption and integrity protection: in the banking business in general. Use link layer encryption and end to end encryption data encryption strategy, the upper using an encryption algorithm which is easy to implement, the underlying hardware uses complex encryption algorithm to protect data in transit security. While for Internet banking, online transmission data packets is based on transaction data structure and Hash Algorithm message authentication code MAC component, the receiver receives MAC verification, and he can detect accidental or intentional data transmission error modified to protect the transmission of data integrity and confidentiality.

(3) Identification and validation: the data source authentication is a means of identification of information. Data source authentication is achieved by digital signature technology. At the same time

using digital signature technology can also achieve the purpose of anti-repudiation.

(4) Network anti-virus technology: including the prevention of viruses, virus detection and removal virus these three techniques. Through these technologies we can prevent the virus goes into the computer system to cause destruction. The latest anti-virus technology should be all of these technologies together to form a multi-layered defense system that has the virus detection, but also has client\server data protection.

(5) Firewall: A firewall is a kind of isolation control technology; in the bank's network and other networks it sets up obstacles to prevent the illegal access to the information, but also can control the banking network to transfer out illegal information.

(6) Monitoring detection. Refers to the process of system access through a variety of technical means to monitor and access behavior and detection, to ensure that the theme of the subject access process's safety.

(7) Audit trails. It refers to the audit, tracking and logging of system, user activity and application, in order to improve the system auditability. System-related activities for a system can have multiple audit trails; records can be stored in the log file and the associated database.

(8) Backup and recovery. It is the security control measures taken by the appropriate technical means, so that make the maximum reduction for the accident on the business impact.

According to bank information security techniques in the eight general protection measures, combined with information security, object hierarchy, the establishment of information security technology system is shown below.

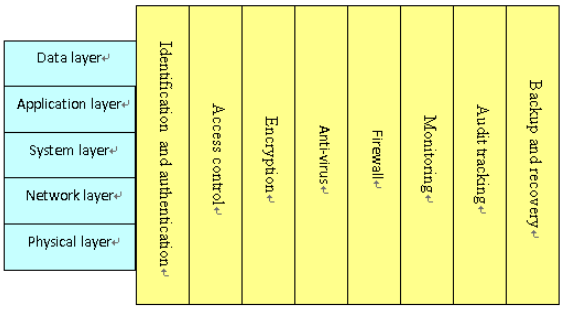

Figure 3: Bank information security technology system.

4.2 Establish Management System to Ensure Banking Information Security

Standardization of information security management system shall be considered from a macro and micro level, macro level mainly refers to the scientific development of the security policies, it reduces the risk areas through standardized information system. Micro level is to make reasonable planning in the system development stage, pre-reduced or eliminated the vulnerability of the system using advanced technology.

(1) Promote the bank information system's technical regulations and standardization, establish and improve the implementation of appropriate monitoring mechanisms, information systems security issues because the ultimate solution to rely on is legal protection. We should speed up banking system's construction indifferent levels, step by step. Especially for online banking, electronic commerce, mobile banking and other innovative products and services, we should match the norms and standards, and establish a scientific monitoring mechanism through the system security, and strengthen technical specifications and standards.

(2) Strengthen the information systems' maintenance and management of daily operations, and gradually establish and improve the documentation of operational processes and make it standardize to ensure the integrity and availability of information.

(3) Establish a centralized monitoring center,

centralize and manage all information, so that monitor the entire banking network, systems and operating conditions at any time, to identify problems and then control the problem through a reasonable process.

(4) Comprehensive use various high-tech means to make interconnection network intelligent. Strengthen the resilience of risk prevention and control capacity to combat financial crimes network to ensure safe and smooth operation of the network system.

(5) Strengthen the banking center and backup data center infrastructure, and ensure the availability of backup systems to reduce and avoid the data risks.

(6) Strengthen training and improve the management and staff's awareness of information security. Particular put emphasis on training operators for information security, making them know the standard and the operate program.

While in the implementation of these management measures we should base on the following three management principles:

(1) More than two persons are responsible: each security-related activity, there must be two or more persons present. For example, access control and recovery with the release of documents, medium release and recycling and disposal of confidential information; hardware and software maintenance; system software design, implementation and revision; important programs and data deletion and destruction.

(2) The principle of limited term: staff should be working in circles from time to time, compulsory leave system, and provides for rotation of staff training so that the limited term of the system is feasible.

(3) The principle of separation of duties: Staffs who work in the information processing system cannot ask others anything which is not concerned with his work unless the leader has approved. Considering security, computer operations and computer programming, the reception and transmission of confidential information; safety management and systems management; application and system preparation procedures, should be worked separately.

5 CONCLUSIONS

Banking computer information system is an important part of national financial information system. It provides financial services to customers. We should put security the chiefly position. The computer network security in bank is a never terminated work which we should keep strengthening the technology and management all the time. In management, security system must be strictly enforced; in technology, network security should be concerned on the emergence of new problems and new technology, constantly block the known security vulnerabilities, and continuously enhanced network security by new technological means.

REFERENCES

Huang Yong, 2008. Based on P2DR security model of bank information security system and design, *Information Systems Management*, Vol. 6, No. 4, pp.115-118

Wood, Charles Gresson, 2005. Establishing Technical Systems Security Standards at a Large Multinational Bank. In *Proceedings of the Third IFIP International Conference*. North-Holland

Sierra, José M., Hernández, Julio C., Ponce, Eva; Manera, Jaime, 2005. Marketing on Internet communications security for online bank transactions. In *International Conference on Computational Science and Its Applications*. IEEE

Kliem, R.L., 2000. Risk management for business process reengineering project, *Information Systems Management*, Vol. 17, No. 4, pp.71-3

Markus, M.L. and Tanis, C., 2000. The enterprise systemexperience – from adoption to success", in Price, M.F. (Ed.), *Framing the Domains of IT Management: Projecting the Future through the Past,* PinnaflexEducational Resources, Cincinnati, OH, pp. 173-207