Research of Information Technology Security in the Financial Industry

XIA Bin, BAI Hui , PAN Bin
Faculty of Business Administration, Xi'an University of Technology, P.R.China , 710054
E－mail: xb611@sohu.com

Abstract

After describing the security condition of the information technology in financial industries, this paper systematically summarizes its basic influence elements on basis of introducing the concept of information technology risks in financial industries，and analyzes relationship of information technology risk factors. Finally, in view of these existence risk factors, guidelines for managing information technology risks in financial industries have been proposed.

1. Security condition of the information technology Analysis

The progress of Information Technology (IT) will most likely continue to accelerate in the coming years. The scope and the reach of computer systems in the financial industry have expanded exponentially. An ever increasing number of financial institutions and related entities are becoming dependent on new technologies for their day–to–day online business transactions and communications. Most offices and households have internet access. By 2005 online banking will rise from 8.5 percent to 50 percent in industrial countries, 1to20percent in emerging markets, and BtoB transactions will become a greater reality [1].Until In June, 2004, there are more than 700 large-medium sized computers in financial industry of China, more than 6,000 minicomputer, more than 500,000 PC server, 63000 ATM, and 4770000 POS (Point of Sales). About 95% network point has realized the electronic. According to statistics of central bank, more than 200 branch offices of more than 20 banks have the website and homepage. Among these, there are more than 50 branch offices with banking online business, the number of enterprise and individual customers exceed 10 million, and more than 100 billion Yuan funds online are in circulation every year.

The computer systems and networks of financial institutions form a significant part of the nation’s critical infrastructure. They are also the prime targets of hackers, terrorists and criminals. As a consequence, IT risks have become more complex and pressing in recent years as vastly more technologies are deployed in the financial industry. Hacker’s attacking to financial network more or more frequently, at present in the global hacker’s attacking event, 40% aims at the financial system, in our country reaches as high as above 60%. In 2001 in USA, there are over 53000 hacks attacking. The magnitude of crimes in USA includes online fraud is 83 times higher than traditional transaction, ＄13billions in losses from computer viruses Code Red and Nimda last year. 57% of hacks are targeted at financial institutions in 2001(IDC).In 2004, in Harbin Heilongjiang Province three college students through online bank of Industrial and Commercial Bank of China, Transfer other’s account fund in own account, steals the bank fund 530,000 Yuan. In 2005 in USA Card Systems database was attacked, and 40 million credit card data were leaked, and 0.2 million cards were steal and brushed.

However, most of the financial institutions have not adopted an approach towards these risks. Businesses do not adequately understand the risks posed by technology, having difficulty identifying them and lack the tools to effectively manage them. According to a recent survey by St. Paul Insurance Companies, only four in 10risk managers have a “fair” to “poor” understanding of technology risks facing their companies; Only 25 percent of companies in U.S.A and 30 percent of European companies have formal management structures in place to manage technology risk; Employees are generally the least informed about technology risks (Provided by Payne Financial Group, Inc.) The situation is more serious in China. The financial institutions in China have not paid enough attentions on this issue, including seldom IT risk management established, no risk assessment and supervision, and few training to employees on IT risk.

This paper tries to make financial institutions aware of the myriad technology risks, the actions they should take to mitigate them, the preparations needed for incidents, etc.

2. Influence factors of information technology risk discussion in depth

Information Technology risks are defined as any potential adverse outcome, damage, loss,

0-7695-3090-7/08 $25.00 © 2008 IEEE
DOI 10.1109/WKDD.2008.55

violation, failure or disruption arising from the use of or reliance on computer hardware, software, devices, systems, applications and networks. These risks are usually related to systems flaws, processing errors, software defects, operating mistakes, hardware breakdowns, systems failures, capacity inadequacies, fraudulent actions and inadequate recovery capabilities. The elements are intended to be used as a flexible tool to facilitate consideration and discussion of the risks associated with information technology.

Information technology risks may results from breaches of policies, inadequate separation of duties, unauthorized access, web-hacking, natural disasters, denial of service, hacking, identity, data center burns, audit oversights, inadequate password administration, systems not integrated, etc. While considering and discussing the risks associated with information technology, there are five information technology elements: Management Process, Architecture, Integrity, Security, and Availability[2]. Although appearing to be most directly related to operational risk, information technology risks also can affect the other traditional risks (i.e., credit, market, liquidity, legal, and reputation) depending on the specific circumstances. Figure 1 shows the risk relationships.

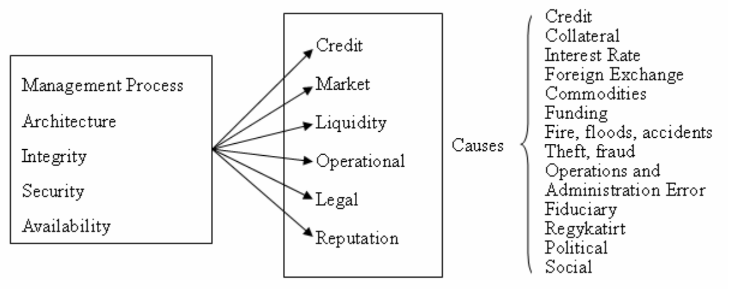

Figure 1 relationship of information technology risk factors

The basic contents of the five elements in IT are defined as below：

Management processes ： Encompass planning, investment, development, execution, and staffing of information technology from a corporate–wide and business–specific perspective. Management processes over information technology are effective when they are adequately and appropriately aligned with, and supportive of, the organization's mission and business objectives；

Architecture ： refers to the underlying design of an automated information system and its individual components. The underlying design encompasses both physical and logical architecture, including operating environments, as well as the organization of data. The individual components refer to network communications, hardware, and software, which include operating systems, communications software, database management systems, programming languages, and desktop software. Effective architecture allow users to easily enter data at both normal and peak processing times, and provides satisfactory solutions to problems that arise when information is stored and processed in two or more systems that cannot be connected electronically；

Integrity：refers to the reliability, accuracy, and completeness of information which is delivered to the end-user. An information technology system has an effective level of integrity when the resulting information flows are accurate and complete；

Security：refers to the safety afforded to information assets and their data processing environments, using both physical and logical controls to achieve a level of protection commensurate with the value of the assets. Information technology has effective security when controls prevent unauthorized access, modification, destruction, or disclosure of information assets during their creation, transmission, processing, maintenance, or storage.

Availability：refers to the delivery of information to end-users. Information technology has effective availability when information is consistently delivered on a timely basis in support of business and decision - making processes.

3 . Management guidelines of information technology security

IT risks are not technical issues but business issues. Financial institutions should strengthen the control ability of technology, enhance internal control, and develop risk management processes according to their risk appetite, security profile and governance culture. The countermeasures for managing information technology risks are proposed as following.

3.1 Technical Control

Each level of entire network system (communications platform, network platform, operating system platform, application platform) all should be taken the safe guard measure and rule by using technology to establish the comprehensive multi-level security system, and provide forceful data security protection, such as data storage security, data manipulation security, data transmission security and data utilization, inquiry and analysis security. Concrete secure measures include identity authentication management, access control technology, firewall technology, and encryption technology.

(1) Identity Authentication Management

The authentication through the distinction and the confirmation of user in the information system, manage the entire process of production, storage, confirmation and maintenance of identity and authentication information. The authentication is the most basic security service. User must pass through the identity recognition in the identity authentication system before visiting system, and then has access to the monitoring equipment. According to user's identity and the authorized database, decided whether the user has access to the resources or not. The general identity authentication includes authentication between the host and the host and authentication between the user and the host. Among them, former authentication mainly based on user's password, smart card and biological feature recognition and so on, while latter authentication based on digital authentication and intelligent discrimination technology and so on.

(2) Access Control Technology

The computer information system activity mainly carries on between the subject and the object. The core problem of financial industry information system security is that guarantees validity access right of the subject to the objects, guarantees the subject access to the object is authorized, and rejects the non-authorized visit to make sure the secret, integrity and usability of information. The access control mainly includes the discretionary access control and the mandatory access control.

(3) Firewall Technology

Firewall is an access control system established in the junction of intranet and exterior network, which filters the information which surmounts the net boundary, in order to work normally when guard against external illegal access, thus set up an electronic barrier for the enterprise. In order to prevented invasion effectively of the illegal user to the network system, two firewalls inside and outside should be established; The inner layer firewall mainly uses to isolate the financial application system to the external access region, and limit access to the internet, in particular to financial industry database system from outside through access region. The outer layer firewall mainly uses for limiting the outside to access host computer.

(4) Encryption technology (key technology)

The data encryption technology which has little effect on the network service and its opening is the primary method to protect the information transmission through the public network and to prevent the electronic interception. At present private key and public key are often combined in the network transmission, to protect the integrity and confidentiality of data of various systems, and enhance the anti-denial of application system service and the data accessing.

3.2Internal Control

The perfect internal control may effectively reduce harm which caused by the internal personnel morals risk, the system resources risk and the computer virus. A set of effective system should be established from every aspect such as the software and hardware management and maintenance control, the organizations and agencies and personnel's management and control, the system environment and the operation manages and control, protection and control of documents, computer virus's prevention and elimination and so on, so as to guarantee the safe operation of financial industry network system.

3.3 Establish function department for managing networks risks

The IT department of a financial institution is originally responsible for main aspects of the firm’s computer, communication, and information processing systems. With deploying technology wider and wider in institutions, IT department becomes a more critical focus area. Many tasks executed by the department are related to the organizations’ mission, business objectives and strategic planning, to the boards and senior management. A new specialized risk management department/committee is needed, who focus on assessing and managing various risk policy, governance issues, organization and implementation.

3.4 Nurture a risk awareness culture

Everyone in the institution should be encouraged to identify and report risks and threats to management so that proper assessment and appropriate actions can be taken. A proactive attitude towards risk control should be fostered. It would be difficult to control risks effectively if the prevailing culture is to deny their existence and employees are generally hampered by the "shoot the messenger" syndrome. Risk disclosure and assessment should be conducted in a rational and analytical manner, without exaggerating or trivializing them.

Financial institutions should advise their customers on how to protect the confidentiality of their information when accessing the institutions' systems, products on how to provide clear and succinct information to them about the risks and benefits or using the services, publish their customer privacy and security policy. Customer dispute handling, reporting and resolution procedures, including the expected timing for the institution's response, should also be clearly defined. Disclosure of the information should be useful in assisting the customers to understand the IT risks.

3.5 Assess and manage Networks risks

The assessment process is a series of steps focused to identifying and managing IT risks, which are including：（1）Identifying the critical business lines of functions that reply heavily on automated systems; (2) Identifying the risks to these business lines; (3) Rating the risks periodically; (4) Reviewing in relation to business objectives.

A comprehensive evaluation of the institution's risk status should be conducted at least once a year or more frequently if mayor systems changes have taken place during the year. This should include a review of the institution's risk policies, risk control processes, incident response procedure, rapid recovery capability and disaster recovery preparedness.

As no computer system is indestructible or infallible, the need for contingency preparations and rapid recovery capability is obvious. Recovery and business resumption priorities should be defined. The incident response procedures and recovery plan should be tested periodically and updated as and when major changes to the business and operating environment occur.

References

[1] WB, 2003：”Electronic Security：Risk Mitigation in Financial Transactions", World Band Financial Sector Report：October 2002

[2] FRS, 1998：”Assessment of Information Technology in the Risk – Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations (SR 98-09)", Federal Reserve Bank of New York, 1998

[3] Wesley Shu; Strassmann, Paul A. Does information technology provide banks with profit?" Information & Management, Jul 2005, Vol. 42 Issue 5, p781-787

[4] ECBS, 1999：”Electronic Banking", European Committee for Banking Standards, October 1999

[5] Susan V. Scott, "IT-enabled credit risk modernization：a revolution under the cloak of normality", Accounting Management and Information Technologies, October 2000.