

<http://ansinet.com/itj>

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSI*net*

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Influencing Factors and Control of Management Information System Security in Furniture Enterprises

Qiumei Zhang

Central South University of Forestry and Technology, 410002, China

Abstract: Under the drive of the booming development of information technology, some furniture enterprises construct Management Information System (MIS) to acquire competitive advantages. But automated data information seems more vulnerable in the face of destroy, fraud, error and abuse. When a computer system is not able to operate as required, the furniture enterprises that depend excessively on computer might encounter serious impacts. This research was conducted by literature research method to determine the influencing factors and control of MIS security in furniture enterprises. Generally speaking, the factors including hacker attack, computer virus, natural disaster, operational error and system defects will influence management information system security in furniture enterprises. The control methods of management information system security in furniture enterprises mainly has the three ones of general control, general control, internet security technology of furniture enterprises.

Key words: Management information system, security, influencing factors, control, furniture enterprise

INTRODUCTION

With widespread use of information technology, more and more furniture enterprises begin to apply computer management information system. Management information system concentrates the data information in a computer file. A large amount of capital is input through computer network each day and confidential information and financial information are stored in the database which become the target of industrial espionage and burglars. However, modern communication technology makes remote control burglary thousands miles away become possible (Wei, 2010). With popularization of computer, people who get a mastery of computer knowledge are on a daily increase and some of them are able achieve a purpose not to be divulged with the information technology they master. Thus, automated data information seems more vulnerable in the face of destroy, fraud, error and abuse (Dong and Guo, 2008). When a computer system is not able to operate as required, the furniture enterprises that depend excessively on computer might encounter serious impacts. The longer the time when a computer system encounters a problem, the larger the losses it brings to furniture enterprises.

INFLUENCING FACTORS IN MANAGEMENT INFORMATION SYSTEM SECURITY IN FURNITURE ENTERPRISES

Hacker attack and computer virus: Explosive increase of use of internet has always been accompanied by rapid

growth of incidents of security damage. The main source is undesirable invader or hacker who employs the latest technology to thrust themselves into a safe computer, stealing information, or destroying data or making them in paralysis. A hacker is a person who enters a computer network without being authorized for the purpose of profit, illegal damage or personal entertainment (Yang, 2003). The potential threat of a hacker to a computer network is appalling. The behavior of spreading computer virus by a hacker has received attention by a large majority of furniture enterprises. Extra software programs are spread rapidly from one system to another which hinders computer storage or damages the programs and data.

A computer virus is a group of computer instructions or program codes that are compiled or inserted in a computer to damage the computer functions or damage the data in the computer and to affect use of the computer and that are able to replicate themselves. A computer virus has a particular self-replication competence. A computer virus can be spread fast and is often difficult to be eradicated. They are able to attach themselves on all sorts of files. When a file is duplicated or is conveyed from one user to another, the computer viruses will spread together with the file. For the time being, there have been more than 30 thousand kinds of viruses. What's more, 200 kinds of new viruses or more are being produced each month. In addition to the path of computer network, a virus can also invade a computer management information system from external resources and "an infected" disc, an infected machine, a software file or an e-mail attachment

that are downloaded on the internet. The potential enormous loss caused by a computer virus has, throughout, been a serious menace.

Furniture enterprises are able to employ anti-virus software and mask program to reduce the possibility of being infected by virus. Anti-virus software is a peculiar software which is specially designed to check the computer system and hard disk that contain a variety of computer viruses. Usually, a software is able to exclude a virus from an infected area. Nevertheless, when the software is red-in, a large majority of anti-virus software can only be effective to the viruses that are familiar to the public. In order to protect their system, the managers have to continuously upgrade their anti-virus software.

Natural disaster: Computer hardware, program, data file and other devices might be damaged by natural disasters, electricity interruption or other disasters. Reconstruction of destroyed data files and computer programs might spend a lot of time and funds and some data lost might not be found forever.

Fault-tolerant computer system contains particular hardware, software and power supply elements which are able to support system backup and avoid system fault so as to maintain running of the system. Fault-tolerant computer contains particular memory chip, processor and disk storage device. They are able to use particular software program or self-check logic to set up their own circuit system and to detect hardware fault and automatically convert it to an alternate device. Components and parts of these computers can be moved and repaired instead of damaging the computer system.

Furniture enterprises can use fault-tolerant technology in the critical application system which has a large quantity of online transaction processing requirements. In an on-line business processing system, the computer is able to immediately deal with online input business. A variety of changes, such as, database, report or requirement for information, may take place in an instant. However, so long as the data are stored, in time, in a medium that is immune from a disaster damage, the data are safe. Furniture enterprises should not long set up their own backup device but, in some cases, have to fall back on a disaster recovery (such as, recovery of disk data) companies.

Even in the daily management process, furniture enterprises should also prevent themselves from property losses caused by all kinds of natural disasters, such as, fire disaster, flood, erosion of aqueous solution, earthquake, tornado, landslide and rainstorm. Computer system is also likely to be exposed to the threat of these disasters. Thus, it is necessary to try to protect the

system from damage of these disasters. Disaster prevention, disaster control and disaster recovery should be taken into consideration in design of safety. For example, the disaster prevention plan ought to contain usage of reserve power supply or particular building material, site testing and drainage system or the measure of structure modification to avoid being damaged in the flood, rainstorm, fire disaster and earthquake. The disaster control plan ought to take into account of the sprinkler systems for fire protection, smoke detection system for fire protection or the waterproof ceiling for preventing water leaching of the fire-prevention pile when a fire disaster occurs. The disaster recovery plan should also take into consideration of how to recover or update operation rapidly after a disaster.

Operational error: A common negligent administrative management or awful computer employee training might both lead to a most common threat. For example, an employee is supposed to format a floppy disk in the Driver of Disk A. however, due to his negligence, he formats the hard disk (such as, original file, Disk D or Disk E of data) of the computer system. As a consequence, the content of the hard disk will be destroyed and important data of the furniture enterprises may be lost beyond retrieve. An employee might input an incorrect number on the screen of data input and then this number might be added, subtracted, multiplied, divided or used in a lot of other programs. As a result, the system might composite and amplify this mistake at an alarming rate.

The computer might also provide wrong service as a wrong instrument. This mistake may be made in a lot of places with circular processing, such as, data entry (where the error of operation occurs), software program mistake, computer operation failure and hardware damage, etc. When the situation is serious, such a mistake will not only interrupt and destroy the records of a furniture enterprise and operation of the enterprise but might also give rise to other immeasurable losses.

Minor errors and defects in the system: A hidden mistake or defect of program code is a primary problem in management information system. The research shows that, as a matter of fact, it is impossible to eradicate all mistakes in a large program. Complexity of decision making code is a major source of minor mistakes. Even a relatively small program that contains several hundreds of rows of statements might also contain a couple of decision-makings that lead to hundreds or thousands of different paths. Usually, important programs of a large majority of companies are large as they contain tens of thousands of rows of codes, so each large program has

more times of choice and more different paths than a small program. The research shows that approximately 60% of errors detected in the test are caused by the norm of designing files. These designed files are usually not complete. It is unlikely to attain the objective of total quality management activity with zero defect in a large program and an overall test is simply not possible, as an overall and one hundred percent of test contains tens of thousands of programs of choices and paths which will take thousands of years. Before a product gets itself proved after it has run for quite a long period of time, even a strict test is unable to precisely confirm whether this system is reliable. We may not eradicate all errors in the information.

Issue of quality of data: The most common source for failure of management information system is bad data quality. Inaccurate and untimely data or data inconsistent with other information resources may cause serious management and financial problems to furniture enterprises. When these data with bad quality escape from being noticed, they might lead to wrong decision making, production returning and even financial loss. Just think that if the furniture enterprises do not have high quality data about their customers, it is absolutely impossible that they are occupied in competitive marketing and customer relationship management.

Likewise, the issue of quality of data also perplexes the public management department. For instance, in US, a research on the criminal record system of computers in the Federal Bureau of Investigation (FBI) finds that, altogether 54.1% of records in the system of the national criminal information center are inaccurate, ambiguous or incomplete. 74.3% of records in the system of the semi-automatic recognition and identification department in FBI show significant quality issues. It is also discovered that 11.2% of guarantee in the files of the automation bondsman of FBI is invalid. A research by FBI finds that 6% of guarantee in the files of all the states in the country is invalid, while 12000 guarantees are approved each day all over the country. The FBI has taken measures to correct these errors but the low level data quality of the system distorts the original meaning of the data. In addition to being used in legal implementation, the cybernated criminal historical records are being more and more applied in public and private departments to screen employees. A lot of these records are incomplete. Although they can show the record of arrest, they are unable to show the punishment record of the court. That is to say, these data are unable to show the evidence of conviction or crime committing. On the

contrary, a lot of individuals may be refused by their employers and thus lose their jobs as these criminal records exaggeratedly describe their criminal behaviors.

CONTROL ON SECURITY OF MANAGEMENT INFORMATION SYSTEM IN FURNITURE ENTERPRISES

General control: General control refers to control over design, security and computer program usage and control over security of the data files which often run through furniture enterprises. In general, general control is applied in all computer operations and is constituted by a composition of system software and a manual program that is able to produce an overall control environment. General control is an overall control to ensure effective implementation of programming procedures and is applied in all application fields. General control contains, (1) Control of implementation which runs through the implementation process of a system, (2) Control of software, (3) Control of physical hardware, (4) Control of computer operation, (5) Control of data security and (6) Control of administrative discipline, standard and procedure, etc.

Control of implementation: Control of implementation is to investigate the development process of the system at different points so as to ensure control and management of the process is correct. Investigation of the system development should search and locate at formal checking points at different development stages of the system, as these checking points are able to let users and managers carry out effective control. Investigation of the system development should also check the level of users' participation at each stage of implementation and cost/profit methodology in establishing feasibility of the system. The investigation also contains development, conversion and test of program and thorough system, user and quality guarantee technology of operation document, etc.

Control of software: Control is quite necessary to different sorts of software that is applied in a computer system. Control of software monitors application of system software and holds back entry of unauthorized software program, system software and computer program. System software is one of the most important areas in control as it performs the function of overall control over direct processing of data and data file.

Control of hardware: Control of hardware ensures that hardware of a computer is physically secure and it also

checks breakdown of the equipment. The hardware of a computer is supposed to be secure physically so that it can only be entered by an authorized individual. The computer equipment should be fire protection, high temperature prevention and moisture-proof. The furniture enterprises also have to prepare backup for emergency in case any electricity interruption and other disasters occur. Quite a lot of varieties of computer hardware contains the mechanical device to check a equipment failure, such as, odd-even check, validity check and "echo check", etc. Odd-even check is able to detect the equipment failure which is responsible for changing the internal bit of a byte in the process of processing. Validity check monitors the structure of the internal switch bit of a byte so as to ensure that a specific computer mechanical device with certain characteristics is valid. "Echo check" determines whether the performance of a hardware equipment is fine.

Control of computer operation: Control of computer operation is applied in work of a computer department and helps to ensure that the programming procedure is consistent and is applied correctly in data storage and data processing. It contains control over the working device of computer processing, control over operation software and computer operation and control over backup and recovery program that deals with abnormal termination.

A responsible staff is supposed to thoroughly record, review and accept working instruction of running a computer. Control of operation software contains design of manual programs used to impede and detect errors. The manual programs are able to develop special instructions for backup and recovery so that wrong changes will not take place in the recovery production process program, system software and data file in the system when hardware or software fault occurs.

Control of data security: Control of data security ensures that the valuable business data files on a disk or an audio tape will not be influenced by any unauthorized entry, alteration and damage. When data are input through an online terminal, entry of unauthorized input has to be prohibited. Control of data security can be developed at the following several levels:

- A terminal is manually restrained so that only an authorized individual can use it
- System software may contain a use password which can only be distributed to an authorized individual. Without a valid password, any person is unable to log in to the system

- For particular system and application, we may design extra password device and security limit. For example, data security software can restrain entry of a specific file. It can set restraint on the type of entry so that only an authorized individual is entitled to alter these particular files. Other people can only read the files (read only) instead of editing or altering them

Control of administrative management: Control of administrative management is a formalized standard, rule procedure and control discipline used to ensure that the furniture enterprises can correctly implement and carry out general control and application control. The most important administrative management controls include, (1) Isolation of functions, (2) Policy making and procedure and (3) Monitoring.

Isolation of functions: Isolation of functions means that the work function should be well designed to, up to the hilt, reduce errors or risks in manipulating assets of furniture enterprises. An individual who takes responsibility for the system in operation is supposed not to be the same person who is able to launch a transaction to make assets changed in the system. In a typical system design, the management information system department of furniture enterprises only takes responsibility for data and program files, whereas a terminal user takes responsibility for the transaction launched (such as, payment and cheque).

Policy making and procedure: The policy made and procedure set up a formal standard that controls operation of management information system. The procedure has to be formalized when designated and has to be authorized by an appropriate managerial level. In this authorization, responsibilities and obligations of the one authorized have to be explained explicitly.

Monitoring: Personnel monitoring which involves control procedures should ensure that control over management information system is carried out in accordance with the purpose. Without enough monitoring, even a best designed set of control might be distorted, misunderstood or neglected and the effect of security of control might, of course, be given a big discount.

Application control: Application control is to apply detailed and precise control for each computer, such as, wage schedule, accounts receivable and processing of an order, etc. It includes automatic and manual procedures. These procedures ensure that only authorized data can be

completely applied or precisely processed. Control of each application is supposed to run through the entire process of the whole data processing. Application control can be classified into, (1) Control of input, (2) Control of processing and (3) Control of output.

Control of input: Control of input is to check correctness and completeness of data when the data enter the system. Detailed and precise control contains such aspects as input authorization, data conversion, data editing and error handling. Input of resource files that flow to a computer has to go through appropriate authorization, recording and monitoring. Input has to be correctly converted to computer data. When it is converted from one type to another, no error is allowed. It is likely to exclude or reduce errors made in transcription to directly input the data into the terminal of a computer through a password or to use the form of automatic control by some resource data. The technologies of input control that are often used contain the following several kinds:

- **Check of rationality:** The data have to fall within a certain kind of restraint that is set in advance. Otherwise, they might be refused
- **Check of normalization:** The system should check the feature and length of content and symbol of personal data, etc
- **Check of existence:** The computer makes a contrast between the reference data input and the data in the table and controls the file to guarantee that what it uses is effective code
- **Check of relevance:** The computer checks whether a logic relationship exists between similar data. If there is no such relationship, it might be refused by the subsequent processing

Control of processing: At a period of renewal, control of processing sets up complete and correct data. The major control of processing includes total amount of operation control, computer matching and programmed copyreader and checkout, etc., such as, programmed copyreader and checkout. A large majority of copyreader and checkout happens in input of data. However, certain applications calls for rationality check and relevance check in the renewal. A typical case is that the management department of furniture enterprises may use consistence check for financial checking and checkout. For example, the electronic billing of the administrative expenditure of a department this month is compared with the billing last month. If the billing of this month is found to be higher at a stipulated value than that of last month, then this billing will be refused and will not be handled temporarily until this billing is checked again.

Control of output: Control of output ensures that the outcome of computer processing is accurate, complete and sent out approximately. The typical control of output contains, (1) Total amount of balance output and total amount of input processing, (2) Browsing the processing record of a computer to verify whether all computer work is approximately carried out or processed and (3) Normative procedure and output report on document introduction and normative procedure to check authorization of key documents, etc.

Internet security technology of furniture enterprises: Joint of intranets and extranets with the internet or transmission of information calls for particular security measures. Public network (including internet) is more fragile as, in reality, it is open to any one and it will receive huge and extensive attack when it is abused. When the internet becomes part of the public network, the management information system of furniture enterprises might be damaged by external behaviors. The computers that are often jointed with the internet are more difficult to prevent penetration from outsiders because they are more and more willing to use a fixed internet address. Therefore, they are more likely to be identified by outsiders and take corresponding actions (Zhu and Wu, 2004).

Firewall technology: Quite a lot of furniture enterprises have employed the Firewall technology so as to hold back any unauthorized user from entering the internal network of the furniture enterprises. Nowadays, firewall has become a kind of necessary measure for internet security. The firewall is usually placed in the internal LAN and WAN or between external networks, such as internet. The firewall takes control over a visitor who enters the internal network of the furniture enterprises through an agency who is similar to a “doorman”. Before allowing a user to enter the internal network, the agency needs to verify the qualification of each user. In the meantime, it also checks whether the information goes against the entry rule carried out by the administrator. The firewall holds back any unauthorized communication from entering the network and allows the furniture enterprises to make a security policy for the traffic between their network and the internet.

As a matter of fact, there are two major kinds of firewall technologies, namely, agent and regular inspection. The agent holds back those data in the firewall that originate from an external organization, checks them and allows them to enter the other party of the firewall through the agent. If an external user intends to have a conversation with an internal user of the furniture

enterprises, the external user needs to, first of all, “have a talk” with the application system of the agent and then the application system of the agent can have a conversation with the internal computer system of the furniture enterprises. Likewise, a computer user within the furniture enterprises has to “have a talk” with external computer through the agent. Since the actual information hasn’t been transmitted through the firewall, the agent is deemed more secure than regular inspection. However, an agent has to do a lot of work which consumes resources of the system and reduces performance of the network.

In the regular inspection, the firewall scans each data file package incoming and checks its resource, target address or service. It sets up a formal table to track information of multiple file packages. The user entry rule defined has to identify each type of file package that the furniture enterprises don’t allow. Although the regular inspection consumes fewer resources than the agent, in theory, it is not quite secure as some data can still pass the firewall.

In order to produce a good firewall, it is necessary to formulate and adhere to an internal rule which is able to identify a person, application or a specific address that is allowed or refused to enter. The firewall is able to prevent but not totally, network penetration from an external user. And it ought to be deemed as one of the important elements in the overall security plan.

Encryption technology: A large amount of furniture enterprises rely on the “encryption” technology to protect the sensitive information transmitted on the network. Encryption is to encode information to make it irregular so as to impede any unauthorized entry or to comprehend the data being transmitted. We can employ a secret digital coding termed as secret key to encrypt the information so as to make the information transmitted as an irregular letter set (this secret key is composed by a lot of letters, numbers and symbols). In order to be read, the information has to be decoded (make it regular) with a matched secret key. There exist a lot of encryption standards. Secure Sockets Layer (SSL) and Secure Hypertext Transfer Protocol (S-HTTP) are both protection protocols which transmit information securely through the internet. At a secure website meeting, when they communicate, these protocols allow customers and server computers to manage encryption and decoding activities. There are several kinds of selectable encryption methods. For the time being, encryption of “public secret key” is relatively popular. Encryption of public secret key uses two different kinds of secret keys, one private and the

other public. These secret keys are correlated mathematically so that data encrypted with one kind of key can only be decoded with the other kind of key. In order to send or receive information, first of all, communicators create coupled private and public secret keys (Zhang, 2003). The public secret key is stored in a catalogue, while the private secret key has to be stored secretly. The sender encrypts the information with the public secret key of the receiver. When receiving information, the receiver decodes the information with his own private secret key.

Encryption seems especially useful in protecting the information of furniture enterprises on the internet and on other public network as the public network is far less secure than the private network. Encryption helps to protect transmission of data. For example, the digital signature on the credit card is one of the applications. Digital signature is digital coding affiliated on the information electronically transmitted and is used to verify the source and content of the information. Digital signature offers a method to link information and the sender together and plays a role similar to written signature. The receiver of the data is able to use digital signature to verify who is sending the data and that the data after “signing a name” is not altered.

Besides, digital certificate is affiliated on the electronic information to further consolidate the certification. Digital certificate system uses a well-known third party as Certificate Authority (CA) to verify the identity of a user. CA verifies a digital certificate that demonstrates the identity of an off-line user via telephone, e-mail or appearance. The information is input into a CA server which produces an encrypted certificate which contains the information of user identity and copy of the public secret key of the user. The certificate proves that the public secret key belongs to a designated customer. CA publishes openly the key he can use or publish it on the internet. A receiver of encrypted information uses the public secret key of CA to decode the password of digital certificate affiliated on the information and verifies it is sent out by the CA. then, he obtains the public secret key of the sender and the certified information contained in the certificate. With this information, the receiver is able to send an encrypted reply.

REFERENCES

- Dong, C.L. and S.S. Guo, 2008. The research of ERP reconfigurable mode based on the theory of evolution. *Manuf. Autom.*, 6: 15-18.

- Wei, L., 2010. Analysis of the enterprise management information system development method. *Enterprise Guide Rep.*, 2: 63-64.
- Yang, H., 2003. Research and development of key technology in manufacturing informatization. *Manuf. Inform. Eng. China*, 6: 4-7.
- Zhang, S., 2003. Where is the way out for informatization of manufacturing industry? *Manuf. Inform. Eng. China*, 8: 4-9.
- Zhu, J. and Z. Wu, 2004. The vision and key technology of manufacture information engineering in furniture manufacture industry. *J. Nanjing For. Univ. (Nat. Sci. Edn.)*, 1: 77-80.