The software environment risks

Business, Accounting

Enterprise information systems to improve business efficiency, but also to all kinds of enterprises to increase the risk of hidden benefits.

All types of commercial enterprise network security-related reports have been emerging, systemic risk issues, and network security issues become increasingly serious. This paper will analyze and propose countermeasures in business information systems, network security risk. Information security risk analysis 1 . The system hardware environment risks “ Hardware is the physical embodiment of an information system.

It is one of the main elements which creates the information system cycle” (n. Operational of business information systems depends on the particular hardware environment, such as various types of databases and web servers, CAN, INTERNET, bank POS terminals, etc. These environments rely on a large number of hardware devices that have a failure rate. When failure occurs, it will inevitably affect the normal operation of information systems.

Failure often occurs mainly in electrical machinery and other aspects of hard faults. These failures of hardware are more frequent. . The software environment risks After the commercial implementation of enterprise information, systems inning various operating systems like database engines, finance and other applications, all kinds of network protocols and communications software. As a software system, undetected errors are inevitable able that could cause confusion accounting, data damage, as well as the compatibility of software Systems and other risks.

Risks are difficult to predict and detect, even after running a longer period test, errors are still difficult to find. . Network of environmental risk As the

information technology developed, the Internet is the greatest technological innovation. Currently, almost all applications for commercial enterprises built are based on network systems, such as financial systems to online trading, logistics management, and e-commerce. Internet has become an important method to enhance the service quality of enterprise and. A large number using of network applications also brings a lot of risks, such as hackers, viruses, and so on. The network environmental risks in information systems of enterprises are facing the risk accounted for the largest proportion.

These risks including hacker attacks, data tampering, and viruses bread, worms, spasms flooding, leaks sensitive information (Opaque, 2013). 4. Information Management Risk Some companies only focus on computer applications in information technology business, and too much emphasis on the service functions of technology, thereby neglect the computer security management and ignore regulatory. Therefore, the network security operation and management, password management specialist, operator management and data management backup media needs to be improved. The business information system security countermeasures For the above listed the risk business information systems, to propose the following preliminary strategies: 1 . The hardware environment Hardware security is a prerequisite for enterprise information system security.

Computers and network equipment should be regularly maintained and save keep records. For unexpected accidents, enterprise should establish contingency plans. To have a person or department responsible for enterprise information system to ensure all equipment are running its best.

In fact, the hardware safety failure caused by natural environment or equipment is not often.

Therefore, the key to ensuring the security of the hardware is to control the human factors, enterprise should focus on strengthening the management of a variety of equipment use and maintenance. 2. The software environment First, the company should do well in system design, such as the using of what kind of operating system, database engine. Thoroughly tested software before it put into use and timely correct software defects.

In addition, companies should strengthen operators' permissions and password management. Assign permissions to people who can access the database in order to enabling authority level control and prohibit unauthorized operation. The company should also change the password periodically and make data backup to ensure data security. Information security policy is the set of rules, standards, practices, and procedures that the company employs to maintain a secure IT system.

This policy can contain items such as when and how an employee should access Secure information and how Often their passwords should be changed (Peggy, 2011 Important data should be backed up and stored in different places to provide solutions to prevent unforeseen failure o that fast recovery program can ensure the integrity of data and information. 3. The network environment Basic requirements of network security are confidentiality, integrity, available, controlled and dubitable. From a technical perspective, the security system of enterprise network systems should include: the operating system and database security, encryption

technology, network security access control, authentication, attack monitoring, firewall technology, anti-virus technology, backup and disaster recovery. From a management perspective, enterprise would focus on a sound management system and operating procedures, enhance staff management, continuously improve employee safety awareness and responsibility, and establish a good troubleshooting response mechanisms.

. Information management Relate to other areas, management of information security of enterprise is often the most easily ignored; however, it is the most important. Managing security is directly related to a variety of security issues that can be effectively prevent and resolve, maintaining security is on the main line and the basis for enterprise information system security management. Among the many elements of the management, the human factor is the most important and most critical and the most difficult to control. Therefore, enterprise must do for people management, strict control of human factors occur. “ Where there are employees who feel that the least security standard is not sufficient, additional security measures must be available” (Bedlams, 2001). Enterprise needs to build information risk prevention system.

Enterprises should pay attention to information security, and set up a department that responsible for information security. Referring to the information security risk management development situations, risk management has become a global information security hot spot, many countries and relevant international organizations all contribute a lot to this field and have made tremendous useful explorations (Dad, 2012).

CONCLUSIONS Enterprise information systems security is a systematic project, involving computer technology and network technology, and management aspects. Meanwhile, with the extension of information systems and emerging technologies integrated application upgrade, it is a dynamic process of mutinous development.