Research on the Security Strategy and Technology of Information Resource Network of Chinese Academy Library

Donghua Zhou
Library, Jianghan University, Wuhan, HuBei, 430056, China

Abstract. This article briefly analyses the Security Strategy and Technology of Information Resource Network of Chinese Academy Library. At present, every country in the world is paying very close attention to the management of library Information resource network (IRN). Library Information Resource System is an important part of the information technology category. There are many risks in the library's information resource system. In order to provide the users with the information accurately and timely, we need to develop a reliable and stable defense strategy.

1. Introduction
Library is a huge information base, and information resource is the foundation of library. The security of library information resource is the main link of the normal operation and development of digital libraries, and is also a guarantee for Library's smooth and safe service for readers everyday. With the efficient use of university library information network, the research development and practice of library information network security, storage technology and related information has been closely combined, which emphatically focus on security problems. But with the development of computer networking and the increasing amount of information in the network use, a variety of advanced security problems pose a serious threat to the information data security. As the degree of automation in library daily management is not very high at present, and the technical force is rather weak. Therefore, it is an arduous task to ensure the safety of the library's information resource network.

2. The Importance of Information Network Security Maintenance in Library
In modern society, computer network has been widely applied in libraries. There is a big security risk process in the library computer network, there are both internal security risks and external security risks, once the computer network security has a emergence, it will affect the operation of the whole system, it is not conducive to the development and utilization of library resources, and is very easy to dampen readers' interest and enthusiasm. For the library, we can see the convenience that the computer network brings to us, at the same time, we should also be aware of the problems of computer network security, and the importance of network security maintenance work, we should pay more attention to maintaining the operating environment of the computer network and the maintenance of network system security, so as to ensure the stability and safety of the operation for the library information system and in order to provide a better information service for the readers.[1]

3. The Factors That Threaten the Security of The Information Resource Network in Library

3.1. The natural disasters and environmental factors
Natural disasters, including floods, fires, earthquakes, lightning strikes and other problems which can cause the damage of computer network. The probability of such problem is relatively small, but it will
lead to large-scale system failure and data loss. The environmental factors mainly refer to the working environment of the library network servers, that does not meet the corresponding requirements, such as power supply, temperature, dust accumulation and other environmental factors and problems.

3.2. The virus infection and hacker attack
The computer virus is a program which is artificially made and is hidden in the data resources of the computer system and can be propagated by self-replicating. In general, when the computer is infected, the data will be damaged and lost. The virus has now generally been made use of destructive activity by means of network communication. Because of the characteristics in the operation of the network itself, it is very easy to achieve rapid propagation. For the library, it lightly interferes with the normal operation of the library, seriously destroys the data and even destroys the whole system of the computer hardware system.

Hackers are mostly engaged in the work of programmers, and have a very deep understanding of the computer operating system and programming language. For the library, if it is eroded there will be serious consequences.

3.3. Computer system defects
Security vulnerabilities are problems in many operation systems. Some system problems are caused by their operation system itself or application software. So, the operation system and software update their version frequently, to improve and remedy the holes and vulnerabilities, but due to various reasons, new vulnerabilities and holes will appear unceasingly, and generate new security risks, if vulnerabilities and holes are not timely repaired, these vulnerabilities and holes will be exploited by hackers, and make illegal intrusion. But sometimes, lots of security risks are due to users themselves. In the library computer network management, it will cause mistakes to the management, and give criminals chances to sneak into the system, resulting in library system destruction and damages.

3.4. Management problems in the Library
Management is the most complex and unsafe issue in the whole library computer management system, because the problems depend not only on managerial staffs, but also on the completeness of the network system itself. For the computer system, the system is not perfect, it can be destroyed by intentional or unintentional destructions. Intentional destruction refers to low moral readers or staff who use the computer to steal books or make virus interference and damage to the operation system. The unintentional destruction refers to low professional qualities staff who make operational errors which cause the loss of data, or staff who is lack of safety awareness that make wrong operations which lead to system failure.

3.5. Computer network technology and management problems
The normal use of computer network and the good use of computer functions require professional computer technology to support it. Only strong technology can maintain the function of the computer and ensure the normal operation of the computer. However, the security problem of the computer network system caused by the technical problems of the computer is the main problem that exists at present. The staff of university library network security management is lack of professional knowledge of computer, also mostly did not receive professional computer training, not related to the sense of crisis on the computer, the computer network technology and the lack of knowledge maintenance knowledge, without a good grasp of the operating technology of computer network hardware, not a safe and effective device and technology management equipment. Can discover and deal with security issues, but cannot play the safe operation of the network security technology to ensure the library network. Due to the lack of corresponding technology of technical personnel, resulting in a hidden danger in the network, which makes library computer work unable to run normally, which is a common phenomenon in libraries.
4. Network Security Technology and Strategy Implementation Purpose in Library

4.1. Technology of computer network security in Library
The security technology of the library computer network means to improve the security of the computer network in the library by taking a series of security management measures. For example, we should guard against the problems of computer software system, and the damage of the hardware system, so that it will not be destroyed by the external operation factors of the library computer network system. At the same time, the library computer network security technology can also effectively avoid important information and data loss in library system. In this way, the library computer network system can operate and serve in a relatively stable and secure environment.

4.2. Computer network security strategy implementation purpose in Library
The library computer network system is a tool to provide users with services and information collection. The goal of network security policy is to protect the integrity and accuracy of these information resources, and to resist the threat of hackers and all kinds of computer network virus attacks. The main purpose of the implementation of the security strategy of the library computer network system includes the following aspects.
- When library users need information, library computer network system must provide users with timely and reliable services at any time.
- The library computer system must practicality and effectively solve the actual information needs of users.
- The library computer network system and the information must be complete and reliable. It is an important goal of library business.
- Libraries and librarians must ensure the safety of these information and prevent malicious use of illegal intentioned people.

5. The Library Information Resource Network Security Strategy

5.1. Set up hardware, software and data management system
In order to effectively prevent the invasion of computer viruses, libraries should made some feasible management systems, including the safety management system of the computer room, magnetic media, disks, and the examination and approval system for hardware outsourcing. These systems can ensure the management of the equipment by special person, so that the operation records can be made for system failures and register, and maintain regularly, maintain timely, and maximize the elimination of computer viruses.

5.2. Library information network access and authority control
The so-called network access control means to control the time and method of the user's login and access to the net by means of technical managements. User’s Access control of network can be divided into three steps: user name recognition and verification, user password identification and validation, user account default check. The user can't enter the network as long as any of the three rules of defense is not passed.

The authority control of the network is a protective measure that is taken against the illegal operation of the network. Prescribed network users and user groups are granted certain privileges to specify which directory, sub directory, files and other network resources can be accessed. It can control what the network users can perform on these directories, files, and network resources.

5.3. Directory level security control
The library computer network system should allow users to access directories, files, and other network resources. The privileges authorized to the network users at directory level are valid for all files and subdirectories. Users can further specify access rights to subdirectories and files under the current
directory. The access rights to directories and files usually include: system administrator rights, read permissions, write permissions, create permissions, delete permissions, modify permissions, file search privileges, access control privileges. The network administrator should specify appropriate access rights for the users, which control the users’ access to the server. The effective combination of these access rights can make system work effectively, and successfully control the access of users to the server resources, thus it strengthens the security of network system and server.

5.4. Library computer network data backup strategy
Software and hardware failure, accidental or malicious use of Delete or Update code statements, destructive viruses, natural disasters (such as fire, floods, earthquakes, etc), act of theft can cause data loss. In order to minimize the loss of data and restore the lost data, it is necessary to manage the database safely and backup the data regularly. RAID technology is recommended for data backup. RAID (redundant array of Independent Disks) is a disk system composed of multiple disk drives (arrays) that treat the disk array as a disk. The RAID device allows data to expand on the RAID strip set, and physically place the database on the corresponding disk drive of RAID, enabling more read/write heads to read data at the same time. Therefore, the use of RAID technology ensures data security and data parallel operation, so as to improve database performance, and users can replace failures without shutting down the system.

6. Conclusion
The security of the computer network management system of the Library is of great significance. Digital library computer network security management is a systematic project, which requires the library management staff all work together, and constantly improve the anti-interference ability of the system to the external environment, and improve the factor of safety, which can provide a safe and reliable digital library management platform for users. In order to ensure the security system, we should actively mobilize resources and formulate scientific and reasonable defense measures to ensure that the computer network management system can be free from the harm of threat.

References
[1] Li Yiqiu; The Digital Library Resource Information Service Efficiency Research[J]; Chongqing Library and Information Science Research; 2009(01):31-32.
[2] LIU Zhi-fang (Zhejiang College of Finance and Economics, Hangzhou 310012, China); Service of established rules to the individualized retrieval under the environment of network[J]; Journal of Academic Library and Information Science; 2006(05): 64-67+93.
[3] LU Hao-dong, ZHANG Jie (Hezhou Institute, Hezhou 542800, China); The risk prevention of knowledge sharing in the university libraries[J]; Journal of Academic Library and Information Science; 2010(01): 49-53.
[4] Zhang Xiaolin; Digital Information Organization: Framework and Technology (Part Two), [J]; Journal of Academic Libraries; 2001(05): 19-24+91.
[5] Liu Jianping Huang Hongwei Li Zuohua (Xiangnan University, Chenzhou 423000, Hunan, China); Studies of Library Virtual Reference Service under the Network Environment[J]; Library Work in Colleges and Universities; 2006(01): 53-56.
[6] Cao Shujin, Luo Chunrong, Ma Lixia; On the Personalized Library Services[J]; Journal of Academic Libraries; 2005(06): 52-58.