Journal of Contemporary Educational Research

Review Article

Security Management Measures for Library Computer Network

Jie Li

Zhongyuan University of Technology, Zhengzhou, Henan, 450007, China

Abstract: Informationization and automation are important in library management due to the development of computer technology and network technology. Although computer networks bring great convenience and improvement to library management's efficiency and quality, there are many security issues that could tag along with networks. The library information is prone to leak due to virus and hackers as well as the transparency of the network. Thus, this leads to a high security risk in library management. Therefore, this paper mainly analyses the security management strategies of library computer networks.

Keywords: *Library, Computer Network, Security Management, Countermeasure*

Publication date: July, 2019

Publication online: 31 July, 2019

Corresponding Author: Jie Li, daoyizhenggu@163.com

1 Introduction

The advent of the information technology age has led to an increase in the number of software, facilities and an increase in information construction. The development of informatization needs to work along with network technology and computer technology. Thus, if a network has high transparency to the public, it leads to many security risks. Computer networks have been widely used in library management. However, if a computer network is maliciously attacked, it will lead to a large-scale network failure, affecting a smooth development of library work and eventually threatening the library literature. Therefore, it is necessary to ensure a tight security of the library computer network.

2 Analyzing problem found in library computer network security management

2.1 Influencing factors of library security

The factors that affects a library computer network management can be divided into two categories as, human and physical factors. The human factor refers to the invasion of the library network caused by humans, which leads to computer network security issues. As an example of human factors, managers that are lack of professional literacy and has difficulties to manage when they are faced with external temptations, malicious attacks, information theft and tampering on computer networks[1]. At the same time, the negligence of library managers can also lead to the disclosure of information and increase the hidden dangers of library network security management. Secondly, physical factors refer to network security management in terms of venues and physical isolation, including the anti-theft system or access control of library hosts. Once it is stolen, these systems will cause severe hidden dangers to the information security of the library[2]. In addition, the power supply of the equipment room also needs to ensure its safety and protective measures to prevent damage caused by voltage shock or sudden power failure. Plus, the surrounding environment of the equipment room, such as dust, temperature, etc., will also have a certain impact on the life and safety of a computer.

2.2 Computer security

The security problems of the computer may lead to the leakage of library management information. As an example, the computer system that is infected by

viruses and system loopholes. Secondly, a computer system's vulnerabilities is a very common problem in a library system management, mainly due to the software itself or operator operations. Computer systems will lead to vulnerability in the process of repairing or software updating. If these vulnerabilities cannot be fixed on time, it will lead to serious security risks and transparency to be attacked by hackers[3]. Moreover, when a computer is infected with virus, the virus will self-replicate and spread onto the entire system of a computer. Plus, the virus is usually hidden in the computer system and it is difficult to find. Therefore, once a computer system is infected by a virus, it causes data corruption and loss or automatic transmission of information to the public, which will affect the usual operation of the library and the working procedures of the computer. At the same time, the computer will then be more vulnerable to more hackers. This situation essentially refers to the invasion of the library network by the external network. Most of the hackers are programmers with strong abilities and familiarity with computer systems and programming languages. Through computer system vulnerabilities, they invade other people's computers, destroy and tamper through illegal means[4]. Therefore, if the library's computer system is attacked by hackers, it will cause the library to face serious information threats, such as the destruction of orphaned books or confidential data leakage.

Table 1. Factors affecting the network security management

Library Security Factors	Human Factors	Physical Factors
Reasons	1. Operation error 2. Vicious assault	1. Environment setting 2. Fire prevention measures
Harms	Loss and tampering of network information	Destruction of network information

3 Library computer network physics and information security countermeasures

3.1 Ensure the physical security of library computer network

At present, computer networks are gradually integrating in all aspects of society. The user components are becoming more diverse and various network intrusions and attacks are also happening more frequently. The library contains many important collection information resources. Once it is leaked, it will cause serious losses. Therefore, it is necessary to ensure a tight security of the library computer network[5]. Firstly by focusing on the physical security of the library computer network, computer network equipment and preventive measures for accidents are mastered to protect the library computer network from the impact and damage of these accidents to ensure the security of information in the transmission and storage of physical media. Physical security mainly adopts the method of physical isolation. It also connects the internal network of the library to the public network and prevents external attacks by hackers through network isolation.

Secondly, it is compulsory to ensure the safety of the venue and environment. It is necessary to set up a anti-theft or access control system in the computer room of the computer network centre to prohibit unauthorized individual from entering the equipment room. At the same time, video surveillance should be set around the computer room to monitor all corners of the computer center. The computer room management staff on duty is responsible to prevent theft of computer network systems at night[6]. Moreover, the network equipment needs to be set up outside the equipment room and the protection reinforcement measures should be improved. It is also necessary to dispatch special personnel to prevent theft of information and equipment in the equipment room. In the setting of the equipment room, it is necessary to avoid some places that are prone to explosions and fires or dark and humid areas. In addition, from the security of the machine room, it is suggested to avoid placing equipment in low-level and top-level positions that are easily stolen.

Thirdly, it is necessary to focus on the management of power and grounding. Computer work must be supported by electrical energy, therefore power protection devices must be installed in the equipment room to protect the computer system with a battery backup in case of voltage shock or sudden power failure. At the same time, the power grounding is also very important for computer protection, which can effectively prevent power clicks.

Lastly, it is important to practice and focus on fire prevention. The computer room must be equipped with an anti-theft system and an access control system and video surveillance should be installed to monitor all corners and important locations of the computer

center[7]. It must be equipped with a fire alarm and fire extinguishing device and an emergency light. At the same time, the staff in the computer room should take in charge of fire prevention and security awareness of the computer room.

3.2 Improving network computer information security management

Network security mainly refers to the security of information including the theory and technology of reliability, integrity and authenticity of network information. Many factors can affect network security include man-made malicious attacks, unintentional mistakes and non-human factors.

Firstly, malicious attacks refer to attacks on computer network systems by malicious people. Then, information stealing and tampering are performed. Malicious attacks can be divided into two situations such as active and passive. Active attacks refer to subjective deliberate destruction of the information computer network system, this is so that the computer network system information is indeed or invalid [8]. While passive attack is worthwhile when the hacker attacks the computer system without stealing the normal work. However, either one, these attacks have an important impact on computer security.

Secondly, human error is one of factors that affect a computer's security. When a network administrator accidentally leaks the account or password to others or the confidential resources are shared due to mistakes during the operation at work or in life, the information leaked will result in a severe reduction on the library's network security.

Finally, non-human factors such as the development of computer network information systems becoming more and more powerful with the rapid development of viruses and hackers are also a cause of risky computer security. When there are loopholes in network computers, these will become the target of viruses and hackers. At the same time, software personnel generally set a "back door" in the process of soft design, which also leaves a security risk for the system.

Table 2. Network computer information security risks and causes

	Vicious Assault	Human Error	Non-human Factors
Form	Active and passive attacks	Disclosure password or operation error sharing	Viruses and hackers
Result	Information stolen or destroyed	Loss of information	Information stolen or destroyed

4 Specific implementation strategy of library computer network security

4.1 Improve computer network security management system

The library computer network security management system is an important standard to guide the computer network management personnel's work ideas and behaviors. The staff can be regulated better and the implementation of safety management system can be guaranteed through the improvement of the computer network security management system. After the safety management system is completed, it will be posted in a conspicuous position and the responsibility will be implemented in the system to specific personnel[9]. In a library computer network, data and server are important guarantees. Therefore, it is necessary to strengthen the stability of the library computer network and enhance the security awareness. As an example, it is compulsory to strengthen and backup library data and the setting of confidentiality. Then, pay attention to the improvement of the supervision mechanism of management personnel to reduce the impact of human factors on computer network security which will also reduce errors.

4.2 Importance of environmental management of library computer room

The environment of a computer room directly affects the security of the library computer network. Therefore, it is necessary to manage the computer room environment. Firstly, it is compulsory to ensure that the ventilation of the computer room is smooth and at a suitable temperature. Secondly, the cleanliness of the environment is also one of the factors. At the same time, it is necessary to do keep look of power supply management of the library computer by storing electricity to prevent hardware loss of the library computer due to power outage or voltage instability. In addition, a strict environmental management system is in place to perform regularly loopholes in computer

systems and troubleshooting and timely maintenance of these systems to improve the operational performance and longevity of computer networks. Thus, this also contributes to the reduction of computer costs.

Table 3. Analysis of computer network protection management technical

Protection Technology	Encryption	Firewall Technology	Address Translation Technology	Antivirus Technology	Network Backup System
Protection Method	Encrypt Network Data	Blocking Software and Information	Guarantee Information Privacy	Severing and Clearing of Virus Replication	Information Replication

4.3 Good protection management of library computer network

First of all, the use of network encryption technology is a very important security method and means in e-commerce. Through the network encryption technology, it can make important data in the network encryption and the form of expression is garbled after reaching the destination of the transmission. Then, the information is restored by decryption. As examples, the main security methods for network information encryption are link encryption, node encryption and endpoint encryption.

Secondly, firewall technology is one of the important security in computer networking. Firewall technology mainly prevents network insecurity factors and improve network security. The principle of its work is to block the insecure factors outside the network through the installation of firewall software and all unauthorised visitors are unable to access the network[10]. The firewall is built for a secure combination of different networks and security zones. At the same time, firewall is also the main calibre of cyber security area. It can control the information flow reasonably within the limits of enterprise security policy and has very strong anti-attack capability. The firewall software needs to be maintain the management interface. In the process of management, the security of the design must be guaranteed as this is also an extremely important issue for firewall protection. Moreover, setting up a service port in the network can reduce the design difficulty and management risk as well as connect to the management host through this port. The firewall does not accept access information from other ports, making it impossible for the external network and the internal network host to hack on the communication. Thus, improving the security of the computer network. In addition, the security of the information can be improved by encrypting the communication. In this way, no port is required so that any computer in the internal network can be used as a management host and a corresponding setting is set between the management host and the firewall.

Thirdly, network address translation technology is part of an important protection as the name implies, replaces one network IP address with another. The main purpose of the design of the network address is to increase the number of addresses, but also has a security feature itself. As an example, when the internal host is relatively hidden, it make the network more secure. The network address is mainly carried out in two aspects in the process of conversion. The first is network administrator's concealment of the internal network address and second is invalid network address. Network administrator's concealment exist in order for the host to not judge the internal network situation while invalid network address exist because the IP address is lacking. It is necessary to pay attention to the conversion of IP addresses as it is difficult to legally apply for an IP address.

Next is network anti-virus technology. Specifically, network anti-virus technology cuts and clears computer viruses through certain technical methods to prevent infringement of the system. This is a technical form of dynamic judgment of the system, which can prevent and classify viruses in the computer system. At the same time, if there are still similar programs and rules appearing in the computer, it will automatically be considered as a virus and then classify it as virus. In addition, the computer virus prevention system is an operation that prevents virus from invading the system and the disk effectively.

Lastly, network backup system is one of the most important safety measure. The storage of information in the network is carried out by means of data. The data can be divided into the category of intangible property; once it disappears, there is no trace, therefore it is necessary to do have a network backup system. The importance of data backup has gradually become recognized with the popularity of computers. Backup refers to the recording and storage of daily business and related files in other locations. However, if the network is flawed, it is difficult to restore the network to work

normally through data backup. The network system backup itself is a complicated and difficult to recover work.Therefore, the comprehensiveness and integrity of the backup must be guaranteed. In a backup system, it is necessary to include data backup and physical fault tolerance of software and hardware so that it can span the entire system. In summary, backups are divided into three forms including full backup, poor backup and incremental backup.

5 Conclusion

In summary, under information technology environment, the problem of library computer network security management has become an important research issue in library management. Therefore, it is necessary to take corresponding solutions according to its specific situation. In the computer network management of the library, whether it is physical factors, human factors, hardware or software factors, it will lead to security loopholes in the library computer network, which will provide opportunities for hackers and viruses to attack. Therefore, library managers must strengthen the analysis of these influencing factors, strengthen the security management of the library computer network, ensure the computer network technology by establishing a sound management system, optimizing the computer room management environment, install and upgraded the defense security system.

References

[1] Alken Geely. On the Application of Computer Network Technology in Library Information Resource Sharing[J]. Digital users, 2018, 24(51):151.

[2] Chen SZ, Teng W, Gao TF. Prevention and Countermeasures of Computer Network Security in Libraries[J]. Network Security Technology and Application, 2017(6).

[3] Tan Y. Ways and Methods of Library Digital Resources Construction under the Network Environment[J]. China, 2017(13):62.

[4] Tu W. Co-construction, Common Understanding and Sharing of Digital Resources in Public Libraries[J]. Yangtze River Series, 2018(2):151–2.

[5] Wan QH, Sun LH. How University Students Adapt to University Life in the Age of Computer Network[J]. Contemporary Education Practice and Teaching Research, 2017(07):234.

[6] Zhang Y. Countermeasures against Computer Network Security in Libraries[J]. Shandong Industrial Technology, 2018, 270(16):232.

[7] Li XX. Countermeasures for Network Information Security Management of Public Libraries[J]. Electronic Technology and Software Engineering, 2017(19):205.

[8] Lu ZC. Discussion on Computer Network Management Measures in University Libraries[J]. Communications, 2017(14):91–92.

[9] Mao ZC. Application Evaluation of Computer Network Technology in Book Management[J]. Intelligence, 2018(14):217.

[10] You GJ. Research on Network Security Threat Analysis and Coping Strategies of County-level Libraries[J]. Network Security Technology and Applications, 2017(8):159.