Discussion on the Technology and Method of Computer Network Security Management

Jianlei Zhou
Baoding Technical College of Electric Power. 071051

Abstract: With the rapid development of information technology, the application of computer network technology has penetrated all aspects of society, changed people's way of life work to a certain extent, brought great convenience to people. But computer network technology is not a panacea, it can promote the function of social development, but also can cause damage to the community and the country. Due to computer network’ openness, easiness of sharing and other characteristics, it had a very negative impact on the computer network security, especially the loopholes in the technical aspects can cause damage on the network information. Based on this, this paper will do a brief analysis on the computer network security management problems and security measures.

1. The analysis of the computer network security problems and causes
With the development of information technology, the state and the community are more a concerned about the computer network security and network information security, the citizen's network information protection attracts more and more attention, and has adopted the relevant protective measures, but because the development time of the network in China is not long, the technical means of network security management is still flawed, the complexity of all aspects of citizen information rights, have caused many problems in China's current computer network security management. It can be summarized as the following five aspects.

1.1 Vulnerability in computer hardware and software
The most important problem of computer network security problem is network information security, the most direct reason caused the damage to information security due to computer hardware and software shortcomings. First of all, there are hidden dangers on the computer hardware, once the computer network hardware equipment is damaged, viruses and Trojans can entered through the hardware into the computer system, the computer network file data and other things will damage, and the virus' spread speed is fast, it is easy to cause the computer system paralyze, resulting in the loss of documents and information resources. As the Trojans and viruses are highly concealed, and the technology is also more and more advanced, so the current protection technology is difficult to achieve foolproof. Second, there are loopholes in computer software, which is due to the negligence caused by the procedural staff in a certain part [1]. Once the software program has problem, hackers and criminals will be invaded into the computer system, attack the computer software programs, programs and systems, cause the computer network security is threatened, making the computer network information get theft and destruction.

1.2 Laws and regulations are not perfect
In fact, China has long been concerned about the computer network information security issues, but also promulgated a number of related laws and regulations, such as 2012 issued "decision on the strengthening of network information protection " has the initial provisions on the protection of citizen
network information, but these similar laws and regulations are only for electronic data which is related to citizenship or citizen privacy, but they are not yet fully related to all personal information, including structured information and unstructured information which is related to citizens. In addition, even in some other laws have the content of citizens on the protection of the right to information, such as administrative law, civil law, but they are only as an additional provision, not in specific measures to implement these laws and regulations, it doesn't define and divide the scope of protection of personal privacy and citizens information rights.

1.3 Industry lacks self-discipline
Network New media era gave the birth to many new media companies, these enterprises are more chaotic in their own management, lack of sense of responsibility. Such as the financial sector industry, some financial enterprises in order to expand their business or for the private interests of some side they do the excessive collection even modify the citizen information, or directly sale the public information. The industry lacks self-discipline, arbitrarily destroys and leaks the information on citizens, so that the right of citizens information is not guaranteed, not only bring risks of the users' property and life who they services to, in fact, it is also harmful to its own long-term development of the enterprise.

1.4 The user's safety awareness and protection measures are not in place
In addition to the objective computer hardware and software vulnerabilities, laws and regulations and industry self-discipline issues, the other one makes the network information security threat is because the user's safety awareness is not in place, they don't take the correct protective measures. Such as login account in the public online, forget to hide the password or choose to remember the password and other actions will make the virus attack personal account easily; for example, fill in important data and didn't use encryption technology to deal with the data, didn't backup the data either, causing the data get lost. The existence of these security risks is because the user does not have the awareness of security, do not pay attention to the protection of personal privacy, fail to grasp the main point of the network technology [2].

1.5 Law enforcement agencies to the crackdown behavior of breaking the network security is not enough
In addition to the objective of the technical reasons which cause the computer network information security risks, the personal subjective security awareness is not strong, there is an another important reason that is in the fight against saboteurs law enforcement agencies did not take effective measures. On the one hand it is due to that the extensive distribution of destructive elements, mobility and concealment are very strong, coupled with their own very high technical means, it enhance the law enforcement departments hunting difficulty On the other hand, because the relevant departments are not in accordance with the national policy of effective implementation, in the fight against sabotage elements, some law enforcement departments don't have strong sense of responsibility, their security awareness is weak, coupled with the need to improve the fighting and other reasons, punishment is still not strong enough. In the supervision of the industry, the relevant regulatory authorities did not strengthen the link between the rows of their own, the responsibility of each other repeatedly occur, the improper management and disorder cause the information of the citizens is leaked, the right to information of citizens cannot be guaranteed.

2. The protecting countermeasures of the computer network information security
In view of the above problems of the computer network security management, I believe that we they should do security management mainly from technical aspects, and then strengthen management in other areas, take reasonable measures to solve the corresponding problems. In the technology mainly use computer security technology to protect and manage the computer network security, in other aspects, strengthen law enforcement and government regulation including legislation, industry self-discipline, individuals should pay attention to protect the network security and personal information security.
2.1 Use computer technology to protect information
The most direct means to protect the network information security is to improve the computer hardware and software, improve the professional level and overall quality of the program staff, technical staff. But any advanced hardware and software will be able to attack the vulnerabilities and have hidden dangers, so in addition to improve the level of hardware and software constantly, but also we need to use computer technology to reduce the risk of attacking network information. The computer security technology mainly in the following (see Table 1). First, use firewall technology in the network of the external and internal barriers. Firewall on the one hand can control the external network data onto the internal network system, make the external data source audit control, on the other hand it can protect the internal data structure, making the internal data is not easily seen by the outside. The control of external data entry and internal data out has played a very good protective effect in order to protect the data security. Second, use the access authorization technology to protect the network information. Access authorization is popular to allow legitimate users to enter the network, the illegal users are refused to go outside the network. To determine whether the user is legitimate mainly through the access, access to passwords, the user identity. Access refers to do the security restriction when the users to be accessed, the user can access only through the inspection, the password visiting is equivalent to the access key, only the password that matches the original password can be recognized by the system and then entered into the internal network. The password must be set to strengthen the settings, otherwise it's easy to be broken. Third, use the intrusion detection technology, that is, all-weather monitoring of intrusion, intrusion detection technology with monitoring, early warning and emergency response and other functions. Fourth, use the encryption technology to protect the user information. Each user needs to learn to use the encryption technology, we also need to increase the difficulty of the secret key, making the outside world will not easily break the protection line. These kinds of computer technology can effectively guarantee the network information security [3].

| Computer technology         | The role of technology                                          | Technical security defense measures                     |
|-----------------------------|-----------------------------------------------------------------|--------------------------------------------------------|
| Firewall technology         | Control external data into the network; protect the internal    | Set up obstacles inside and outside the network         |
|                             | data structure                                                  |                                                        |
| Access authorization technology | Allowing legitimate users to enter the network, the illegal    | Set access, access password, and user identity          |
|                             | users outside the network                                       |                                                        |
| Intrusion detection technology | Monitoring, early warning and emergency response                | Monitor intrusion every day                             |
| Encryption technology       | Protect the security line isn't break by the outside            | Set the cipher key                                     |

2.2 Strengthen and perfect laws and regulations
There is a need to strengthen legislation at the national legal level. In the legislation, we must first clear the relevant legislative principles, in addition to ensuring the safety of computer networks, but also need to develop appropriate laws and regulations in the network security information management, such as computer network security management needs to protect the privacy of citizens, besides the privacy information other information which can be circulated in accordance with laws and regulations, other citizens information must be protected by laws and regulations. Second, we must determine the scope of the protection for civic information and specific protection measures. Because we are going to protect the information on citizens, so which areas and the specific protection measures needs to be protected should be stipulated in the law clearly. In addition, it should establish a clear and complete personal information protection law, so that the information rights of citizens are guaranteed.
2.3 To improve the industry’s self-discipline

The above mentioned in the computer network security, some enterprises or individuals due to their personal interests make damage to other citizens’ interests, free disclosure of citizen information, endanger the computer network security behavior. To improve computer network security, in addition to technical and legal aspects of the method, we also need the joint efforts of enterprises and individuals. First of all, require units and individuals to enhance their own quality, the unit cannot lay out the user's information for the sake of the interests, individuals cannot reduce the protection of user information because lacking responsibility. Second, once the unit organization found that employees have leaked information behavior, they must deal with these kind of behavior severely; individuals need to strengthen self-cultivation ability, improve cultural quality, not be tempted by outside and don't does the act of breaking a law.

2.4 Strengthen government supervision

In addition to set up a clear supervision and management of all walks of life outside, the government also needs to strengthen the guidance of these regulatory management. For example, the CBRC, while monitoring the financial institutions, also should contact with other regulators and strengthen the cooperative relationship, so the government should unified the management, divide the scope of the role to form a joint force. Regulatory authorities on the supervision and disciplinary mechanisms needs to determine which important information of the citizen information and other computer networks cannot be transmitted. Second, it is necessary to strengthen the supervision of new media organizations, so that these enterprises needs to improve the citizen information and other computer network information protection measures. In addition we should also regulate the personal information behavior of the citizens, when necessary, regulate and punish the behavior of citizens.

2.5 Strengthen the user's safety awareness and protection awareness

First of all, users must pay attention to the computer network security and computer network information protection, have a clear understanding of the existence of computer network defects, protect their privacy in a timely manner to prevent the disclosure of personal information, enhance personal safety awareness and protection awareness. For example, don't login personal account in the public network, outside the Internet at random, encrypted to their own information, do not tell the password to others and so on. Only the security awareness is rising, they will take favorable measures to protect the computer network information. Second, the relevant departments should also strengthen the computer network security publicity and education, and guide people use the Internet legally, do not believe that online information and links arbitrarily and have a sense of protecting rights, once found their information has been tampered or leaked, do timely alarm processing to these illegal behavior.

2.6 Strengthen law enforcement efforts of the law enforcement departments, punish disciplinary units and individuals severely

In addition to legislation to improve the computer network security laws and regulations, in law enforcement should also strengthen the intensity of disciplinary units or individuals to severely punish. On the one hand we mentioned in the previous article, some units or individuals do some damage to the computer network security for their own interests, such as leakage of personal information and so on. For this deliberate damage to computer network security behavior, the unit itself needs to recognize the importance of protecting the computer network security, while enhancing self-awareness at the same time, but also the law enforcement departments need to regulate the law. For example, once the unit or the individual in unit makes a similar violation of law, law enforcement agencies required to investigate the unit or individual in accordance with laws and regulations first, and then do the corresponding punishment according to the damage degree. On the other hand, law enforcement agencies must adhere to the principle of fairness and impartiality and openness in law enforcement. Treat any unit and individual in accordance with the laws and regulations of the objective requirements, do not cover and condone, in order to ensure the effectiveness of law enforcement. Such as serious acts of wrongful acts
and lawless elements, developed the clear and specific punitive measures to avoid reduce the punishment of illegal behavior which lack of operational law enforcement measure.

3. Conclusion
With the rapid development of information technology and the network, individuals, society, countries and even over the world all need to pay attention to computer network security, because the security of computer network information is related to personal interests, stable and harmonious development of society, development of economic, technology, culture military and other aspects, as well as the safety of the country. Because once the computer network is destroyed, important network information will be leaked, which will cause extremely adverse political and military impact to the country. Therefore, for the existing computer network security problems, countries, society and individuals can take different means to do computer network information security protection.

References
[1] Li Linteng, Zhao Yizhang. Computer network information security and protective measures [J]. China's strategic emerging industries, 2017 (02).
[2] Chen Dongmei. Computer network information security and its protection strategy based on computer network technology [J]. Electronic Testing, 2017 (03): 131-132.
[3] Cao Cheng, Zhou Jian, Zhou Hong, Wang Mingfu. Network security and countermeasures [J]. Journal of Hefei University of Technology (Natural Science Edition), 2007 (09): 14-16.
[4] Zhai Sujuan, Sun Yuxiu Computer network security management related issues [J]. Coal Technology 2011
[5] Lan Hao. Talk about the computer network security management measures [J] computer CD-ROM software and application 2011