Information Security Risk Assessment and Countermeasure Research of Electronic Commerce

Wei-hong zhou, Fang-dong fan*

Hunan Institute of Traffic Engineering, Heng Yang, Hunan, 421009, China

*Corresponding Author

Keywords: E-commerce, Information security, Risk assessment, Countermeasures

Abstract: in recent years, accompanied by some policies and regulations of the implementation of e-commerce has been rapid development, gradually expand the application field, increasingly rich profit model, at the same time some information security risk, in order to improve the electronic commerce information security risk consciousness and technology, provide a more complete evaluation system.through online and offline investigation and research, this paper analyzes the security problems of e-commerce, and gives some improvement measures.

1. Introduction

Electronic commerce is an electronic commerce activity based on the Internet and based on the logistics of consumer products in shopping malls.When related departments or personnel of e-commerce are developing projects, having a set of information security risk assessment system can help them to analyze potential threats in a scientific and reasonable way and ensure the security of economic system.Therefore, the combination of information security technology and modern emerging technology will For us to create a more high-quality network environment.

2. Information Security Problems and Status Quo in Electronic Commerce System

Generally speaking, the information security of e-commerce refers to the information security that both parties use a variety of technical and legal means in the process of e-commerce transaction to ensure that the transaction will not be damaged by accident, malice or disclosure of these unfavorable requirements.At the beginning of the 21st century, the computer crime rate in China's financial system has been increasing, China's financial network information security situation is very serious, need to strengthen and improve.The following is a brief introduction to the information security issues in the e-commerce network, mainly involving the following aspects:

Because the electronic commerce system software can be written in different forms, it is difficult to avoid leaving security loopholes in the practical application process.For example, the network operating system itself will have some security problems, such as illegal access to I/0, these incomplete mediation and chaotic access control will cause database security vulnerabilities, and these vulnerabilities seriously affect the information security of the electronic commerce system.In particular,The security of TCP/IP communication protocol is not considered before the design, which indicates that there are some avoidable or inevitable security holes in the network software of the current electronic commerce system.There are also risks associated with information sharing.In the process of information transmission, it is necessary to continuously process and reproduce the information source and intercept useful information, which inevitably leads to the risk of information transformation.Especially in the current mode of “social networking + business”, a message may be reproduced on social networking sites for tens of thousands of times or more in an instant. Once there is an error in information reprinting, the impact will be great, and attention should be paid to the risk.

With the wide application of network technology, the problems brought by computer viruses become more and more extensive, compressed files, E-mail has become the main way of the

  DOI: 10.25236/ecemis.2021.033

transmission of computer viruses, because these kinds of viruses are very diverse, highly destructive, so that the transmission speed of computer viruses is greatly accelerated.In recent years, the number of new virus species has increased rapidly, and the Internet has provided a good medium for the spread of these viruses.These viruses can spread in large numbers through the Internet and any carelessness can cause irreparable economic losses.There are also risks associated with the transmission of information.Information is an important resource, good flow performance to maximize the value of information, but in the process of information transmission needs to go through many paths, and in this process there are often some unsafe factors, to bring certain risks to information security.

The current hacker attack, in addition to the spread of computer virus, the malicious behavior of black appearance is also more and more rampant.The Trojan horse makes it possible for black people to use computer viruses to become more purposeful. As a result, the login information recorded by the computer is maliciously tampered with by the Trojan horse program, leading to the theft of many important information, files, and even money.

The security problems of e-commerce companies caused by human factors, most of the confidentiality work is carried out through the operation of employees, which requires employees to have a good confidentiality, responsibility and sense of responsibility and other moral qualities.If the staff's sense of responsibility is not strong, the attitude is not correct, it is easy to be used by others, let irrelevant personnel enter the room at will or leak confidential information to others, criminals can be allowed to abolish important information.If the staff lack good professional ethics, they may illegally change or delete others' information beyond their authorized scope, and they can also use their professional knowledge and work location to steal user passwords and identifiers for illegal sale.

3. Problems Existing in Risk Assessment of Electronic Commerce Information Security

After a large number of data collection and analysis, it is not difficult to find that information security risk assessment is a problem to be solved in the current scientific research work.At present, there are some researches and applications on information security risk assessment in China, but these researches are only simple analysis, including common risk assessment tools with risk.Evaluation matrix, questionnaire, risk assessment matrix and questionnaire method, expert system combination.Further efforts are needed for further exploration.In addition, quantitative factor analysis method, time series model, decision tree method and regression model are commonly used for risk assessment of network information security.Risk assessment methods and qualitative analysis mainly include logical analysis, Delphi method, factor analysis method, historical comparison method, etc.Among them, the combination of quantitative and qualitative evaluation methods is composed of fuzzy analytic hierarchy process (AHP) and evaluation methods based on D-S evidence theory.At the same time, there are still some problems in the risk assessment of network information security. For example, with the development of the network, China has moved from 2G to 4G at the beginning, and now it takes the lead in entering the 5G era.There are also various problems, the number of Internet users Increasing the need to urgently raise their awareness of information security vigilance.

3.1 Lack of Understanding of Risk Assessment of Electronic Commerce Information Security

At present, many relevant personnel do not have enough awareness of the current situation that e-commerce information system is facing great challenges, and lack of experience in information security risk assessment.

Therefore, they do not pay attention to the importance of information security risk assessment for the following reasons.

First, the company or unit of risk assessment has yet to pass the standard test, training standard, research of information security risk assessment work has not been system related theory, method and technology tools, this is due to some relevant information security evaluation of leadership and staff to assess information lack of awareness of the importance of risk assessment, so naturally will

be such a risk assessment included in the framework of the current information security system.

Second, although there are many departments to information security work in an important position, but by human resources, material resources, financial constraints, social system constraints, the lack of policies and regulations make information security system information security risk assessment work can not get due attention.

3.2 Lack of Professional and Technical Personnel in Information Security Risk Assessment

First of all, the technical content of information security risk assessment is very demanding, which requires employees to have a very high technical level. Now many companies use common information as risk assessment technicians.

Second, the information security risk assessment is a comprehensive, professional work, not only involves the company's all business information, also involves human, material and financial resources of all aspects, so you need to the interaction between the various departments, the departments of most companies rely on information, participate in the information security risk assessment of the independent without debate they want to complete the information security risk assessment work is very difficult.

To sum up, training information security risk assessment professional technical personnel is the future direction of information technology development.

3.3 Risk Assessment Tools Are Relatively Lacking

At present, except the expert system, other analytical tools are relatively simple, in addition to the lack of practical theoretical basis.In addition, the development of this information risk assessment tool in application presents the present situation.Indicates domestic and external imbalances and is relatively backward in China.It can be seen that the key to solve the problem of information security is to have mature risk assessment tools.

4. Suggestions on Preventing Information Security and Risks of e-Commerce

4.1 Strengthen the Awareness of e-Commerce Information Security and Risk Assessment

Most information transmission and processing, and people are inseparable.Especially to master the important information of personnel and core business, personnel's personal factors, management factors and environment risk. Mainly including personnel technical ability, monitoring management, security. In particular, it is necessary to supervise and audit companies, ensure that information security risk management is integrated into practice, give full play to the role of internal supervision, and promote the recognition of social responsibility and the implementation of information security risk management. E-commerce companies must conduct necessary information security knowledge education and training for workers, understand the relevant laws and regulations, and do a good job in the secret protection of key customer information. Do not arbitrarily view and disclose customer purchase information.

Enterprises should increase efforts to protect the confidentiality and integrity of information during network communication operations, strengthen key management, improve the ability to respond to network attacks, take measures to avoid overstepping authority or abuse, and eliminate the risks of users in transactions. In the information security risk control, the internal system environment, network boundary and backbone network security must be protected from inside to outside. Establish perfect management system for network information system, and provide comprehensive security guarantee. Use an end-to-end strategy. As there are many kinds of user terminal devices in mobile e-commerce and the security environment is complicated and difficult to control, it is necessary to do a good job of identification in the important link of data transmission. Through face recognition, fingerprint recognition and other technologies to effectively improve the user access identity identification ability, greatly improve the security of the account, to ensure the security of data transmission, to ensure that the real and effective transaction.

4.2 Provide Professional Technical Training to Improve the Skills of Professionals

Carefully choose third-party partners, enhance the level of information management, strengthen performance supervision and management.

Establish a reasonable internal organizational structure and effective fund guarantee, cultivate employees' awareness of information security, create a good working atmosphere for information security, and strengthen the awareness and ability of information security professionals to assess information security risks. Through a large number of experiments, it is found that relevant personnel can be trained through the following methods:

First, carry out information security risk assessment regularly, gather employees together to learn relevant materials, so as to enhance their awareness of information security and make up for existing defects.

Second, special technical training and guidance for the staff of the information security department can improve the technology through simulation analysis;

Third, the company should increase the investment in technical resources, employ experienced experts and scholars to form a third-party evaluation organization, and introduce risk assessment equipment. For a rainy day;

Fourth, the company shall conduct standardized certification training for technical personnel, implement the vocational qualification access system, raise the threshold for technical personnel, and include information security risk assessment and comprehensive quality assurance assessment for technical personnel. The above methods are only simple training methods for specific implementation and possible problems still need to be studied.

4.3 Improve the Research and Application of Information Security Prevention Technology

For mobile database to store the data is encrypted to prevent leakage and adopt different methods of encryption to protect data security, identity authentication, data recovery, data encryption storage, physical isolation, firewall, network, network equipment, network intrusion detection and network vulnerability scanning, network equipment, backup, network management, special line, realize the network management and a series of technical means, so as to improve the security of the database. At the same time to enhance the awareness of the importance of physical facilities, regular maintenance of physical facilities.

In order to monitor the information security and implement the evaluation system, we should ensure the independence of the basic hardware and chips. In the establishment of an evaluation system independent of information security, we should organize important information security technology research at home and abroad, and establish an innovative electronic commerce information security and evaluation system.

5. Conclusion:

Electronic commerce information security is a very complex project, which involves both the transmission of data information and the storage of information. It is not only a technical issue, but also a legal issue. It is a business activity that consumer groups participate in together and its related non-technical issues. Therefore, on this basis, the needed in the information security system to set up a good evaluation system, however, at present our country information security risk assessment has some flaw, this requests us to actively cope with problem, dare to challenge, from information security awareness, professional talent and new technical level, to improve risk assessment standard. Provide a safe and reliable platform for the development of electronic commerce.

References

[1] Wu Pengcheng. Discussion on Electronic Commerce Information Security and Risk Management [J]. China New

[2] Zhao Gang, Wang Xingfen. Architecture of Electronic Commerce Information Security Management System [J].Journal of Beijing Information Science and Technology University, Vol.26, No. 1, 2011

[3] Wu Yongfeng. Security Risk Assessment Method of E-Commerce Transaction Based on Fuzzy Support Vector Machine [J].Science and Technology Bulletin, Vol.28, No.9, 2012

[4] Gao Bo. Research on Electronic Commerce Information Security Risks and Prevention Strategies [J]. Modern Commerce and Commerce Industry, 2011(14)

[5] Fan Guangyuan, Xin Yang. Analysis and Design of Firewall Auditing Scheme [J].Information Network Security, 2012(03):81-84.

[6] Lang Weimin, Yang Depeng, Li Husheng. Research on Smart Grid WCSN Security Architecture [J]. Information Network Security, 2012(04):19-22.