Analysis of the information management level optimization of the information security in E-commerce

Qiumei Hu

School of Information Technology Jiangxi University of Finance & Economics Nanchang, 330013，China

E-mail: hqq_1002@163.com

Keywords: information management, e-commerce, information security

Abstract: In the rapid lead of the economy and information technology, electronic commerce has been developed rapidly. It is triggered a new round of the information security problem of e-commerce, information security is the platform of fundamental business can run smoothly. This article elaborates mainly the E-commerce information security problem from the angle of information management, optimize information management, ensure the safety of information, it is the basic guarantee to accelerate the development of electronic commerce.

1. INTRODUCTION

E-commerce is the promise of electronic payment through the network to obtain electronic products or delivery of physical products. Compared with the traditional business model, e-commerce is based on network and information, therefore, when the information and networking wave the world, electronic commerce also can be realized. The electronic commerce development so far, the key factors that hinder its development is the problem of information security. The network is the space and time, distance barrier, the network transaction information authenticity, security and certainty, legitimacy and effectiveness is important particularly, and the network security present uncertainty directly affects the development of electronic commerce, information security is the most important guarantee to promote the development of electronic commerce.

2. CONCEPTS OF INFORMATION MANAGEMENT

Since the 70's, the term information management was proposed, more and more high frequency. About the conception of "information management”, there are many different interpretations. Although scholars on the connotation, extension and development stage of information management have different kinds of argument, but the concept of information management recognized can be summarized as follows: information management is a kind of strategic management to achieve the organization's objectives and meets the requirements of the organization, planning, and development of information resources, to solve environmental problems the control of the organization, integration and utilization .

The Special information management is to manage information; information is an object of management. This definition, put forward the information management is a multi-level concept, the object of information management not only information, but also includes the person, organization, equipment and environment; information management goal is to effectively meet the information requirements; the means of formation management is through the allocation of resources to achieve its goals. Through the literatures in China and abroad extensively, found that people understanding of information management in the following five different meanings: the information content of information management, media management, computer information management, management information system, the team management information industry or industry.

3. HIDDEN SAFETY PROBLEMS OF E-COMMERCE INFORMATION

3.1 information storage security hidden danger

Safe storage of information refers to the information security of electronic commerce in the static storage. Information storage security of e-commerce mainly as follows: the two aspects of internal and external risks. The computer system is the basic equipment of electronic commerce, if not Caution! Problem, as it would threaten the information security of electronic commerce. A computer device itself physical damage, loss of data, information disclosure and other issues; on the other hand, the computer system also often suffers from competitors malicious intrusion, information spy illegal intrusion and computer virus damage. At the same time, the existing staff management problems of computer system, if not clear responsibilities, unknown permissions will also affect the security of computer systems.

3.2 information transmission security hidden danger

Information transmission security refers to E-commerce in the operation process of logistics, capital flow, and information flow after merged into a dynamic transmission process security. Mainly in the attacker in the transmission channel of the network, through physical or logical means, information interception, tampering, delete, insert. An attacker could intercept, through the analysis of the characteristics of the network physical line transmission, interception of confidential information or useful information, such as the user's account number, password etc.Tamper with, which is to change the order of information flow, change the information content; delete, i.e. delete portions of certain information or information; insert, namely insert some information in the message, let the receiver can’t read or accept the wrong message.

3.3 information security hidden trouble of transactions both parties

The traditional business is face to face; both parties to the transaction can easily build a sense of trust and a sense of security. Electronic commerce flows through the network to achieve the exchange of commodities about the seller and the buyer information, which makes the electronic commerce transaction both sides have doubts in the sense of security and trust degree. Electronic commerce transaction both sides are faced with information security threat: some users may be issued on their own information to malicious denial, to shirk their responsibilities. Such as: information promulgator denied ever sending a message or content, denying the editor of data processing; the recipient later denied having received a piece of information or content; buyers make order does not admit; commodity quality and description of merchants sell does not match but not admit etc..

3.4 information security service reject

The attacker makes information, business or other legitimate resources access blocked. Mainly for spreading false information, disrupt the normal information channel. Including: false website and store email, to the user to subscribe to manifest; fake ads, a large number of users, e-mail, business resources exhausted, that legitimate users can not normally access to network resources, so that, there is time critical services can’t be timely response.

4. THE SAFETY FACTORS OF E-COMMERCE INFORMATION

From two aspects of security and trust in the traditional view, transaction process, both sides of the transaction is face to face, therefore, to ensure the security and trust relation transaction. But in the electronic commerce process, both sides of the transaction is to contact via Internet, as e-commerce relies on the network has the characteristics of dynamic, virtual, highly open, making e-commerce facing threat and security risks, many therefore, transaction security and trust between

the two sides quite difficult. The safety factor of e-commerce is mainly reflected in the following aspects:

4.1 information security

E-commerce as a means of the trade, the information directly represents the personal, enterprise and national commercial secrets. Traditional paper-based trade is through the mail package mail or by sending a commercial message communication channels and reliable to achieve the purpose of confidentiality. Electronic commerce is based on a more open network environment; commercial anti leak is an important guarantee for comprehensive application of electronic commerce.

4.2 information validity, authenticity

Electronic commerce gets to replace in electronic instead of the paper, how to ensure the validity and authenticity of this form of electronic trade information is a prerequisite for development of electronic commerce. Electronic commerce as a form of trade, the validity and authenticity of the information will be directly related to the individual, enterprise and national economic interest and reputation.

4.3 information integrity

Electronic commerce makes the process trades simplify, to reduce human intervention, but also bring the problem maintenance of unified business information integrity. Because the data input of the accidental error or fraud, differences may lead to trade party’s information. In addition, the order of difference, information loss in the process of data transmission repetition or information transfer can lead to different parties to trade information. Therefore, the electronic commerce system should fully guarantee the data transmission, storage and electronic business integrity check is correct and reliable.

4.4 information reliability, controllability

Reliability requires that information can guarantee the legitimate and resources of the use is not improperly rejected; do not deny that the requirement is to establish the responsibility mechanism effectively, prevent the entity to deny its behavior; controllability requirement is to control the person or entity to use resource use mode. In the traditional trade, trade both sides through a handwritten signature or seal in the trade contract, contract or trade documents and other written documents to identify trading partners, to determine the reliability of contract, contract, and documents and prevent denial behavior.

4.5 authentication

Network environment is a virtual environment, and the electronic commerce is carried out in this virtual platform, both sides of the transaction generally do not meet, need to have the technology and the corresponding strategy to carry on the authentication. When an individual or firm showed identity-commerce services provide a kind of identity authentication methods to determine the legitimacy of the identity, to ensure the identity of the users.

5. OPTIMIZE THE MAIN IDEAS OF INFORMATION MANAGEMENT

5.1 The physical security of the information

Network security must first solve the problem is to ensure the physical security of network. Physical security is the information dissemination in the network media the safety. Physical security is the basic safeguard information security, is an indispensable part of neglect and. Strategies of

physical security is designed to protect the computer system and the communications link from natural disasters, man-made damage and attack. Ensure that the computer system has a good electromagnetic compatibility work environment. At the same time to make the perfect and safe management system, and prevent unauthorized access to computer control room to do all kinds of theft, sabotage. Suppression and prevent electromagnetic leakage, is another major strategy problem of physical security. At present the main protective measures has two kinds: one kind is the protective conduction emission. Another kind is the protection against radiation.

5.2 information encryption strategy

Encryption technologies is the most basic measures of e-commerce, initially mainly used and ensure confidentiality of data in storage and transmission in the process of. With the development of electronic commerce, puts forward new requirements for data integrity and identity authentication technology, digital signature, identity authentication is to meet the need of new technology and new application derived in cryptography. Encryption technology is a kind of active information security prevention strategy, the use of encryption algorithm, the plaintext into meaningless cipher text, prevents illegal users to understand the original data, to ensure data confidentiality.

5.3 information authentication

Authentication is an important technique to prevent active attacks, it is important for the safety of all kinds of information system in an open environment. The main technical certifications are: first, the sender authentication information is true, rather than pretending, this is the entity authentication; second, message integrity verification, and this is the information certification. At present, only the encryption technology is not enough to guarantee that in the electronic commerce transaction security, identity authentication technology is to ensure that an important means of e-commerce security technology. The certifications include digital technology, digital signature, digital envelope technology, digital time stamp technology and digital certificate technology etc.

5.4 information security protocol

Present, there are a variety of security in electronic commerce system can guarantee the security of electronic commerce transaction, where SSL and SET are the two most important protocols in electronic commerce security. Secure socket layer protocol (Secure Socket Layer, referred to as SSL) is a kind of protection Web communication industry standards, the main purpose is to provide secure communications services on the Internet, is a special key sequence cipher encryption technology and RSA based on the strong public key, to credit card and personal information, electronic commerce provides strong encryption protection.

5.5 safety quality information personnel

The unsafe factors and some are inevitable, such as natural disasters; some are factitious. For the safety of man-made factors, the most important point is to strengthen the training of personnel quality, the first is the cultivation of computer human qualities, so that no "hacker", no Trojan program; followed by "deny". The second is to cultivate the electronic commerce the quality of people, the two sides do transaction integrity, including commodity information, functional information and transaction information is not ambiguous etc.

The problem of information security is probably more embodied in the management. A considerable part of the current system for energy through physical contact the user to provide the back door, so that users forget password can enter the system, therefore, in order to ensure the information storage security first should strengthen management, avoid personnel without physical contact system authorization, malicious damage, to prevent the system transplant virus, opened the back door etc.. At the same time to authorize physical contact system personnel should also assign

permissions strictly, control user access to directories, files, equipment assign permissions to ensure the safety of electronic commerce information.

6. Conclusions

Safety is the core and soul of the electronic commerce. Electronic commerce information security always is a problem of concern; therefore, how to solve the problem is the motive force to promote the better and faster development electronic commerce. However, because of security problems are constantly changing, so the solution security problem means is will continue to change. At present, propose the electronic commerce also has many new technologies, but not form an effective and safe electronic commerce system, it need to intensify our efforts to the research and development of information security technology, to build a secure business environment.

References

[1] Zhao Bin, Research on Third-party E-business Model for Small-and-Medium Enterprises [J], China Logistics & Purchasing, 2009 (14), pp.67-68

[2] Angela Baby. The electronic commerce security problem analysis [J]. China information technology science, 2005 (20).

[3 Xia Jing. Study on e-commerce communications security [J]. Science and Technology Information Development & economy, 2005 (15).

[4] Angela Baby. The electronic commerce security problem analysis [J]. China Science and technology information, 2005, (20): 53

[5] Wang Dongwei. Discussion on thee-commerce information security [J]. Computer knowledge and technology, 2006, (23): 73-74.

[6] Yan Cuiling, Wang Wen. The security of electronic commerce in [J]. digital signature technology modernization of shopping malls, 2007 (13)