International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp. 153-162
http://dx.doi.org/10.14257/ijsia.2014.8.3.17

Research on e-commerce Security based on Risk Management Perspective

Wu Yanyan

School of Computer and Information Engineering
Harbin University of Commerce, Harbin, China
wyyhrb@163.com

Abstract

Electronic commerce can help enterprises reducing costs, obtaining greater market and improving relationships between buyers and sellers. At the same time, new risks and threats have also occurred, such as, mutual trust, intellectual property, network attacks and so on. This paper analyzes the threat classification and control measures, and on this basis, a conceptual risk management framework is provided. Enterprises engaged in e-commerce can use the framework to improve their security.

Keywords: *e-commerce; security issues; threat classification; risk management*

1. Introduction

E-Commerce is getting more and more popular with customers due to the ever-growing number of companies that provide business to consumer e-commerce services (electronic business transactions between businesses and individual consumers who are buyers).

One of the critical success factors of e-commerce is its security. Without the assurance of security, e-commerce may not work normally. And it is a complexity issue, because e-commerce security relates to the confidence between sellers and buyers, credit card and extremely sensitive personal information. Therefore, the security of e-commerce depends on a complex interrelationship among applications platforms, database management systems, software and network infrastructure and so on. Any single weakness can jeopardize the e-commerce security. A. Sengupta *etc.*, viewed the security of e-commerce as an engineering management problem and examined the issues from a life cycle approach [1]. Fang-Yie Leu etc, studied e-commerce security based on cloud computing, wireless network and they paid more attention to technical approaches to prevent a system from being attacked [2]. Meng Xiangsong *etc.*, focused on the security of mobile agent and the secure authentication infrastructure based on PKI was proposed [3]. Giannakis Antoniou etc. and Rhys Smith etc paid attention to the privacy in e-commerce transactions and provided some suggestions [4, 5]. In addition, the security technology application at multiple levels will slow down the system [6]. Therefore, it becomes critically important to analyze e-commerce security. This paper will analyze the security issues of e-commerce and then put forward a conceptual risk management framework.

2. Security Issues of Electronic Commerce

The rapid development of Internet has promoted electronic commerce explosion. However, at the same time, the internet businesses have brought large security issues such as

ISSN: 1738-9976 IJSIA

mutual trust, intellectual property, and possible attacks to the network. And with the development of electronic commerce, these issues have obtained more and more attentions.

2.1. Mutual Trust in Business

In the traditional commerce, participant can face to face, so there may be little distrust. However, there is difference in electronic commerce. For example, in electronic commerce, the location of the business and the goods are unknown. More important, there is not personal contact between the seller and the buyer. In addition, there is lack of a clear legal framework in electronic commerce. Therefore, how to enhance mutual trust is an important issue.

2.2. Intellectual Property

Intellectual property (IP) is an important legal term that refers to copyright and related rights. It is expected to play an increasing role in the future. Especially in e-commerce, IP is more important. E-commerce is more special than other business systems, because many products and services sold in internet are based on IP, such as music, software, pictures, photos, designs, *etc*. In these goods, IP is the main component of value. And this kind of goods is more suitable to be traded through e-commerce [7]. If there is lack of protection for IP, these goods may be stolen or pirated and even the worst thing, whole business can be destroyed.

In addition, IP is involved in the whole e-commerce work. Internet itself is a product of IP. The systems include software, networks, designs, chips, routers and switches, the user interface, *etc*. All of these are forms of IP and protected by IP rights. In other words, without IP e-commerce may be nonexistent. Similarly, branding and goodwill are essential elements of e-commerce. And they are also protected by trademarks and related laws. So IP management is the foundation of e-commerce.

2.3. Network Attacks

Networks attacks have become a general phenomenon, especially with the spread of e-commerce. And the types of attacks are more and more. Security for e-commerce broadly is related to security of networks and databases. The most common kinds of attacks include:

A. IP spoofing attacks

IP spoofing attacks is the common security issue in the Internet business. That is to say, a hacker steals an authorized Internet Protocol (IP) address. And then the hacker pretends the authority to make a business. This behavior may bring the authority a big problem.

B. Stealing information

In the transaction process, the hacker listens to Transmission Control Protocols/Internet Protocol (TCP/IP) packets. Therefore, the hacker can steal the information of business or some important personal message, such as e-mail messages, credit card numbers and so on.

C. Password attacks

Most users use passwords to control the system, such as e-mail, bank account *etc*. So password is the common target of hackers. Hackers generally find a user who has an easy password [8]. If a hacker obtained the system administrator password, the whole system is in dangerous.

D. Social engineering attacks

There are many users who have little understanding their computer system. And they are the aim of the attack. The hacker sends an e-mail message to the users and asks for their password is a typical attack.

E. Vulnerable technological attacks

The system typically the operating system allows a hacker to access the system normally is attacked. A typical one is for the user to gain access to a system. And the user may run an intensive program which can slows down the system.

F. Trust-access attacks

The typical attack is that a hacker adds its system to the list of systems. As a result, the system can allow others to enter into the system without a user password.

3. A Model for Threat Classification and Control Measures of e-commerce

This part will provide a model to analyze the threat classification and control measures of e-commerce. Firstly, we consider threats from two points of view: threat agents and threat techniques. Then we analyze the security control measures.

3.1. Threat Agents

Threat agents include 3 parts: environmental factors, authorized users and unauthorized users.

A. Environmental Factors

Environmental factors are common sense. It is more prone to certain environmental influences and natural disasters than others in some areas. For example, fire is not geographically dependent. However, tornadoes and floods can be predicted in specific areas. In addition to the natural disasters, the danger of mechanical and electrical equipment failure should be paid to more attention. So is the interruption of electrical power.

B. Authorized users

There are some potential threats when authorized users and personnel are engaged in supporting operations. Especially they exceed their privileges and authorities. It may affect the ability of the system to perform its mission. Personnel should be considered as potential threats, when they have the access to a system or occupy positions of special trust. Because they have the capability or opportunity to abuse their access authorities, privileges or trusts. And it may bring danger to the system.

C. Unauthorized users

An unauthorized user can be anyone who is not engaged in the system. It can attempt to interrupt the operation of the system overtly or covertly. It may sabotage hardware and associated equipment. And it also could be accomplished through the manipulation of software.

3.2. Threat Techniques

Techniques can be classified into 5 types: physical, personnel, hardware, software, and procedural.

A. Physical

It implies to use a physical means to enter into restricted areas, for example, building, compound room or other areas.

B. Personnel

Personnel are the people who have authority or privilege to access a system, either as users or operators. Penetration techniques and methods generally deal with them. Threat agent may recruit them to penetrate the system, operation or facility. They themselves can become motivated to make an attack.

C. Hardware

Attacks using the characteristics of the hardware may involve a physical attack against the equipment, a bug implanted within a hardware controller or an attack against the supporting utilities. The purpose of it is to subvert or deny use of the system [9]. In this category, hardware generally includes any kind of equipment of the system, such as power supplies, air conditioning systems and so on.

D. Software

Software attacks have a large scope from discreet alterations to less discreet changes. The discreet alterations are subtly imposed for the aim of compromising the system. And the less discreet changes intend to bring the result of destruction of data or other system features. Techniques can penetrate the software, application programs or utility routines to threat the system.

E. Procedural

If the system is lack of adequate controls or existing controls are failure, authorized or unauthorized users can penetrate the system [10]. For example, if former employees retained the used valid passwords, unauthorized personnel may pick up output. This is a procedural penetration.

3.3. Security Control Measures

There are some detailed security control measures in the ISO 7498-2 Standard lists. For example, there are involving authentication, access Control, data confidentiality data integrity and non-repudiation. Computer security experts widely accept this classification. And they are also recommended by the authors good control measures [11]. The threat agent, threat technique and security measures are shown in Figure 1.

We can use Figure 1 to classify threats and security measures to confront these threats in e-commerce. For example, access control is one of the security measures. It can face the threats that may be caused by an unauthorized user through hardware. Totally, there are combinations with agents, threat techniques, and security measures. However, not all of these combinations are available. We just utilize this three-dimensional view for a better security risk management.

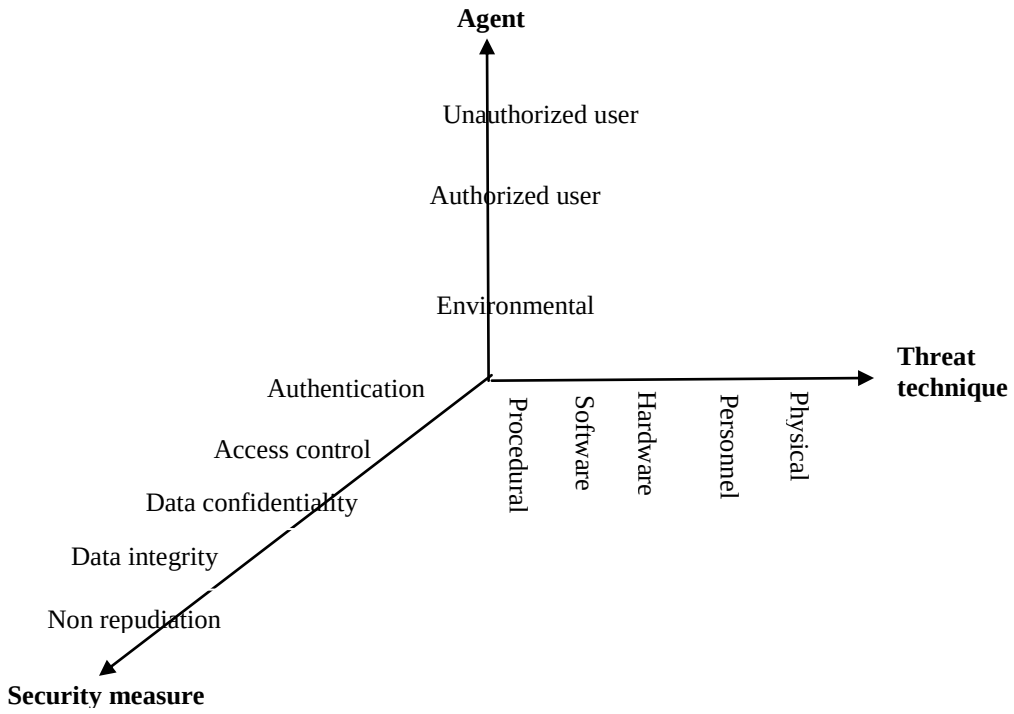

Figure 1. A Model for Threat Classification and Control Measures of e-commerce

4. Quantifying the Cost of Security

To analyzing the e-commerce, it is better to quantify the cost of security. Firstly, enterprises should know the values of assets, especially the assets exposed to the threat [12]. We can classify the logical and physical assets into 5 categories, as following:

A. Information

It involves the documented data or intellectual property. They are used to meet the mission of an organization.

B. Software

Software is the important component of e-commerce system. It can process, store or transmit information.

C. Hardware

Hardware mainly includes information technology physical devices.

D. Personnel

People is the most valuable asset, especially who posses skills, knowledge, and experience. It is difficult to replace.

E. Systems

Systems are a combination of information, software, and hardware assets. In addition it includes any host, client, or server being considered. It can process and store information.

There is an example that a denial of service attack causes the cost of downtime per hour. The loss can be computed as follows:

a) Productivity
It may be calculated by the equal: (Number of staffs impacted) × (hours out) × (burdened hourly rate).

b) Revenue
It can be evaluated by direct loss, lost future revenues.

c) Financial Performance
It can be evaluated by credit rating, stock price.

d) Damaged Reputation
It can be evaluated by customers, suppliers, financial markets, banks, business partners, *etc*.

e) Other Expenses
Except these tangible costs, there are many intangible losses, such as equipment rental, overtime costs, extra shipping costs, travel expenses, *etc*. It can be computed to use scoring tables, as shown in Table 1.

Table 1. A Score Table for Intangible Damages

Intangible damage	Score
Trouble limited in the project	1
Trouble spread to other operating sites	1-3
Trouble spread in the organization	3-5
Open through local news report	5-7
Adverse through national news report	7-9
Tremendous influence on stock price or even bankruptcy	10

Table 1 defines valuation scores for intangible damages. The losses may be caused by an accident. The company can meet various departments and business units or their experts to give the values found in the tables. The expected cost of an incident can be calculated by Equation (1).

$$EC = \sum_{i=1} AP_i \times C_i \qquad (1)$$

Where *EC* is the total cost of the incidents, *APi* is the occurrence probability of the incident *i*, and *Ci* is the cost of damage caused by incident *i*.

5. A Conceptual Risk Management Framework for e-commerce

To contain the complexity and maintain focus and relevance, this paper will restrict to issues related to the security of database and information system of e-commerce [13]. And we put forward a conceptual risk management framework for e-commerce. According to the following five stages, we can firstly identify the vulnerabilities of a company, second evaluate the existing security measures, and then select the most appropriate and cost-effective countermeasures. This conceptual risk management framework is shown in Figure 2.

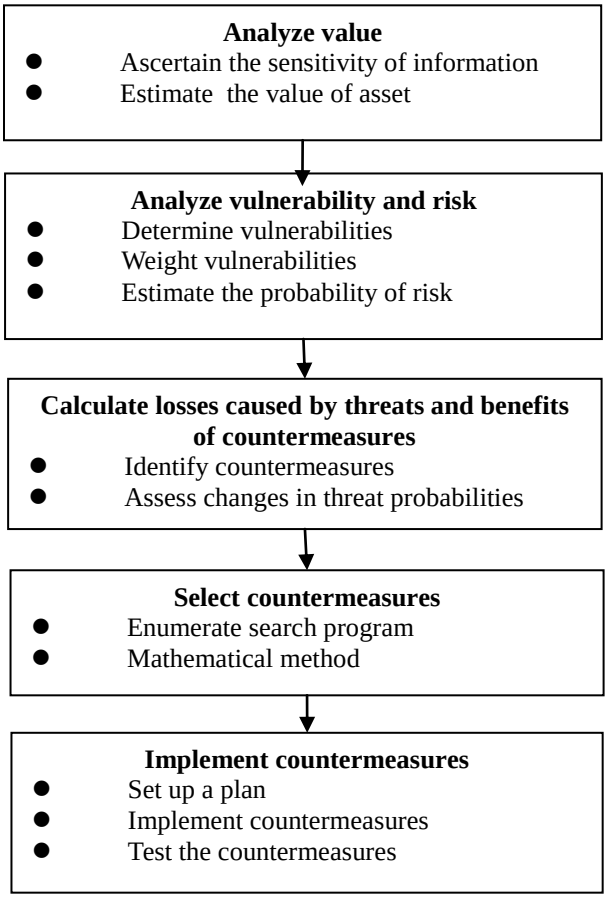

Figure 2. A Conceptual Risk Management Framework

5.1. Analyze Value

The resource and application value analysis can be done in two phases. Firstly, determine the sensitivity of information. It can find the sensitivity level of each application and it is useful to find the most sensitive type of data, such as privacy, asset/resource and proprietary [14]. Therefore, it is important for its detail and accuracy. Secondly, estimate the asset value. The asset involves the resources such as physical facility, equipment and supplies, software and so on.

5.2. Analyze Vulnerability and Risk

This analysis can be divided three parts. Firstly, identify vulnerabilities. Companies must identify the weakness or flaws in the design, implementation or operation of the security controls of a facility or system. It can be done through the analysis of the security measures or the related factors. Secondly, weight vulnerabilities. It should consider the seriousness and potential degree of exploitability to identify the vulnerabilities. Thirdly, assess threat probabilities. The probabilities should be documented.

5.3. Calculate Losses caused by Threats and Benefits of Countermeasures

Enterprises can calculate losses caused by threats and benefits of countermeasures through defining countermeasure at given levels [15]. The cost of the countermeasure at a given level involves its effectiveness, expected damage caused by threat and so on. It also includes the probability that the threat occurs, assessing changes in threat probabilities, expected benefit and loss of countermeasure and so on.

5.4. Select Countermeasures

This stage can be done in two phases: enumerate search program and mathematical method. The aim is to choose a countermeasure to minimize the total cost.

5.5. Implement Countermeasures

This stage includes three phases. Firstly, set up a plan. It is mainly done by the senior management. And they need give the staffs much more encouragement. Secondly, implement countermeasures. It is the key link of the framework. Specific action can be completed in this phase. Thirdly, test the countermeasures. The aim is to ascertain that the proposed countermeasures produce the desired effect. And it does not result bad effects.

6. Conclusions

This paper analyzed the security issues confronted by enterprises engaged in e-commerce. The paper highlighted the role of trust and intellectual property management in e-commerce. At the same time, a three dimensional view of threat agent, technique and control measures are provided to further illustrate the e-commerce security. And in the paper, we also pay attention to the cost of security and give an equal to quantify it. Finally, a conceptual framework is provided to deal with these issues. The framework is just a conceptual idea for enterprises to handle security issues, and further research will continue.

References

[1] C. Mazumdar Sengupta and M. S. Barik, “E-commerce security-a life cycle approach”, Sadhana, vol. 30, no. 2-3, **(2005)**.
[2] F.-Y. Leu, C.-H. Lin and A. Castiglione, “Special issue on cloud, wireless and e-commerce security”, Journal of Ambient Intelligence and Humanized Computing, vol. 4, no. 2, **(2013)**.
[3] M. Xiangsong and H. Fengwu, “Design on PKI-based anonymous mobile agent security in e-commerce”, Wuhan University Journal of Natural Sciences, vol. 11, no. 6, **(2006)**.
[4] G. Antoniou and L. Battern, “E-commerce: protecting purchaser privacy to enforce trust”, Electronic commerce research, vol. 11, no. 4, **(2011)**.
[5] R. Smith and J. Shao, “Privacy and e-commerce: a consumer-centric perspective”, Electronic commerce research, vol. 7, no. 2, **(2007)**.
[6] D. Good and R. Schultz, “E-commerce strategies for B2B service firm in the global environment”, American Business Review, vol. 20, no. 2, **(2003)**.
[7] J. Pathak, “A conceptual risk framework for internal auditing in e-commerce”, Managerial Auditing Journal, vol. 19, no. 4, **(2004)**.
[8] M. Warren and W. Hutchinson, “A security risk management approach for e-commerce”, Information Management & Computer Security, **(2003)**.
[9] G. Eschellbeck, “Active security a proactive approach for computer security systems”, Journal of Network and Computer Applications, vol. 23, **(2000)**.
[10] E. Pate-Cornell and S. Guikema, “Probabilistic modeling of terrorist attacks:Asystem analysis approach to setting priorities among countermeasures”, Military Operation Research, **(2002)** October.

[11] F. Farahmand, S. B. Navathe, G. P. Sharp and P. H. Enslow, "A Management Perspective on Risk of Security Threats to Information Systems", Information Technology and Management, vol. 6, **(2005)**.
[12] F. Farahmand, S. B. Navathe, G. P. Sharp and P. H. Enslow, "Evaluating Damages Caused by Information Systems Security Incidents", Economics of Information Security Advances in Information Security, vol. 12, **(2004)**.
[13] A. K. Ghosh and T. M. Swaminatha, "Software security and privacy risks in mobile e-commerce", Communications of the ACM, vol. 44, no. 2, **(2001)**.
[14] K. Someswar and R. Sam, "A framework for analyzing e-commerce security", Information Management & Computer Security, vol. 10, no. 4, **(2002)**.
[15] C.-S. Lee, "An analytical framework for evaluating e-commerce business models and strategies", Electronic Networking Applications and Policy, vol. 11, no. 4, **(2001)**.