Study on the E-government Security Risk Management

Zhitian Zhou, Congyang Hu

Institute of Policy and Management of Chinese Academy of Science, Beijing, China

Summary
The implementation of e-government is based on information technology, how to solve the security problem of the e-government system is becoming an extremely urgent subject. This paper, from the angle of security risk management, analyzes the procedures of e-government security risk management from three aspects: risk identification, risk analysis, risk control. And the corresponding countermeasures are proposed. Nowadays, with the fast development of information technology; strengthening risk management is an effective way to guarantee the security of e-government system.

Key words:
e-government risk management risk control

1. Introduction

With the popularity and maturation of computer network technology, the real-time sharing of a large amount of government information and the two-way exchange has been already possible technically. E-government is a kind of governmental administration which based on electronic information technology. The essence of e-government is using electronic information technology to break the boundary of administrative organizations, and build up a virtual electronic government. People can get government information and services through electronic media. Governments can communicate with each other through various kinds of electronic media which can be used inside government bodies, between different governments, or between government and society.

However, there are many problems exposed in the spread of computer network technology. Security is the most important one. It was said by National Computer Network Emergency Response Technical Team/Coordination Center of China (CERT) in 2007, they had received 26476 network security incident reports. This is three times more than 2005 which was reported 9122 network security incidents. As a result, with the fast development of e-government; it is particularly important to strengthen security consciousness and take strong preventive measures in technology and management aspects.

On the research of e-government and information security model, Westerlind K., in his master's dissertations [1], proposed that the return of the information technology investment should be evaluated from six aspects: negotiability, contents, quality, adaptability, important degree, and scalability. Theodosios Tsiakis and Geogre Stephansides built a model for information security investment [2]; the models they adopted were mainly from financial models, such as ROI, ALE and so on. Those models were investment profit and loss models. Based on these, they put forward a concept on information security risk control.

Japanese scholars Tanaka, Hideuyki, Matsuura, through their empirical study on Japanese small-scale e-commerce and e-government cases, have proved that the relationships of information, vulnerability, and information security in information communication were in accord with the economic model Gordon and Loeb proposed in 2002. [3] In 2003, Lawrence A. Gordon, Martin P. Loeb and William Lucyshyn have showed the big profits obtained by sharing the security information in decentralized e-commerce or e-government systems through the utility model in economics. This kind of sharing behavior can be promoted by some incentives.

Recently, there has been a very convenient method — E-GOV-OFSR (Organizational Framework for the Security Requirements of E-Government Services), which helped to identify the risk requirements for each business in e-government system. [4] On this basis, Lambrinoudakis, Costas, Gritzalis and Stefanos itemized security requirements for each business in e-government services, and proposed a PKI (Public Key Infrastructure)-based e-government system integrated platform which could meet the above security requirements. They have verified the feasibility of this method through an e-government system case which called “Webocart”. [5] Leitold H., Hollosi A., and Poseh R., through the case of Austrian citizen card implementation, stated an e-government system security architecture which based on digital signature, PKI technology, etc. [6]

Wimmer M. and Von Bredow B. [7] compared e-government with e-commerce, analyzed the security problems of e-government system from technology angle and non-technology angle, and they have proposed the whole solutions for different security requirements. Conklin A. and Whiet G. B. [8] explained the differences

Manuscript received May 5, 2008
Manuscript revised May 20, 2008

between e-government and e-commerce systems in detail, and proposed corresponding models respectively. They suggested an e-government system preview to collect relevant computer security information in order to make sure that the implementation of e-government could meet the public demands.

Kun Wang, Lihua Zhou, Zhen Cai have established a Robust Disaster Recovery System Model (RDRSM). [9] It is applied in the e-government system that is hypersensitive to the information security. Benabdallah S., Gueniara EI Fatmi S. and Oudriga N. B. set up an available e-government security model. [10]

Ji Jianyue, Wang Yuanyue described the development of e-government in our country. [11] They analyzed the problems existing in the development of e-government in China, and proposed relevant development strategies. Du Wenzhong and Ma Liping believed that security problems in e-government were inevitable after analyzing in security, benefits, and costs aspects. [12] They said e-government security was a problem without standard answers; we must avoid to build e-government in swarms. We should handle the relationships of security, benefits, and costs with consideration. Zhang Weihua introduced several problems existing in the establishment of our country's e-government information security architecture. [13] Zhang also presented some relationships we must pay attention to, and some core technological problems we must solve. Ren Jinhua analyzed the status of network security in our country. [14]The present software and hardware technology level in our country is low, it seriously hamper the establishment of e-government security guarantee. In his paper, he has done lots of detailed analysis on the advantages and disadvantages of dominating network security technologies currently, such as firewall technology, intrusion detection technology, and security audit technology.

Yan Qiang and Shu Huaying stated security risks which e-government system faced from the angle of security risk management. [15] Shen Changxiang discussed e-government information security guarantee system from strategy angle. [16]The technical framework of security guarantee system has been divided into three levels and two centers. And he emphasized the importance of security products with independent intellectual properties. Wang Huanxi analyzed e-government information security from the angle of law. [17] In Zhang Chongbin and Suo Yanfeng's paper, [18] they have analyzed some information security technologies at present, such as isolating technology, intrusion detection technology and so on. And they have proposed some relevant application strategies.

In China, e-government is a new thing. The disparity between our country and developed countries is very far not only in theories but also in legal aspect. There are a lot of studies in these aspects. In the study of e-government information security, the focuses are on anti-terrorism and the evaluation of e-government system risks. This paper, from the angle of risks which the e-government facing, analyzes the procedures of e-government security risk management from three aspects: risk identification, risk analysis, risk control. And the corresponding countermeasures are proposed.

2. The E-Government Security Risks

The development of e-government, which is based on internet, meets fatal security problems due to the complexity and vulnerability of network. Generally speaking, the security risks e-government facing includes the following aspects:

2.1 Information Intercepting

It means that the related e-government users or invaders capture or steal the e-information from governments or other users.

2.2 Information Tampering

The internet attackers tamper, insert or delete original data through various technical methods, and transmit them to the destination, in order to damage the integrality of the data.

2.3 Services Denying

It is the complete invalidation of the network system or the servers system in some period. It mainly comes from the attack of the hackers or the virus, and the man-made destruction of the devices as well.

2.4 System Resources Stealing

In the network system environment, the stealing of the system resources is very common.

2.5 Information Faking

It means that after the attackers know the rules of the data in the network information or after they have decoded the government information; they could pretend legal users or make false information to cheat other users. The main forms include pretending users to get illegal certifications, forging e-mails, etc.

3. The Procedures of Risk Management

Risk management is a course which includes identifying risks, analyzing risks, and drawing up risk management plans. The procedures of security risk management of e-government include three steps: risk identifying, risk analyzing, and risk controlling.

3.1 Risk Identifying

The security requirements for the e-government system are confirmed by system evaluations of the risks. Risk identification is the first step of risk management in order to charge the security risks of e-government effectively.

Risk identification is based on the collecting of various relevant threats, bugs and corresponding countermeasures, and then recognizes any possible risks or potential threats to the e-government system.

There are many different kinds of methods to identify risks. The goal of risk identification is to recognize risks existing in network environment, in data or data exchange.

One problem should be noticed is that risk identification can not charge all the e-government system risks. Risk identification can only find the already known risks or potential risks which based on known risks. We use risk analysis and risk control to solve or reduce most other unknown risks.

3.2 Risk Analyzing

Risk analysis, through various kinds of qualitative or quantitative methods, such as analysis, comparison, evaluation, etc. is to decide the importance of each factor of e-government risks, rank the factors, and then evaluate every possible result to the e-government system. Threat is a kind of potentiality which launched unintentionally by threat source, or threat source attacked the vulnerabilities of the system intentionally. It is that the system has vulnerabilities, so threat sources become risks. So in the process of risk analysis, we must identify and describe threat sources.

Threat sources can be any kinds of environments or events include people, nature, and so on, which do harm to the system. The natural threat that system facing relates to its geographical location; however, the threats from people may have no intention or on purpose. To identify threats the system facing, we can use many different methods, such as brainstorming, Delphi, Scenarios Analysis, etc. Table 1 lists some possible threat sources.

Table 1 Possible Threat Sources

Threat	Possible Source
Intentional Threats	terrorists
	people who dissatisfied with the organization, or has a mental imbalance
	criminals
	insiders who colluding with alien enemies
	hackers
Unintentional Threats	mis-operations from system users
	mis-operations from system chargers or protectors
Natural Threats	earthquake
	volcanic eruption
	hurricane
	flood
	thunder and lightning
	hail

We can get the information about vulnerabilities through spot investigation, personnel investigation, network scanning, penetration testing, relative documents analyzing, or other open information sources on vulnerabilities. In the stage of vulnerability analyzing, if the system is still in designing, the emphasis is on the strategies or rules of the system security, and the definitions of security requirements. If the system is already implemented, we should also analyze some more specific information, such as design documents. If the system is in using, we need to do some further analysis, such as the system security functions, actual effects of the security control, etc. For the threats from people whose possible motivations are listed in table 2.

Table 2 Possible Motivations

Motivation
obtaining access privileges of secrets or sensitive data
tracking or monitoring the operations of target system
disturbing the operation of target
stealing money, things or services
using resources without authorization (such as computers, website resource and so on)
technology challenges
curiosity

The ultimate goal of threat analyzing is to calculate the general risk probability. The factors influencing risk probability include motivations and ability of threat source, system vulnerabilities, and effect of relative security measures. Calculating risk probability is a course with very strong subjectivity. There may be some history records about natural threats, those records can help to analyze the probability that natural threats happen. But we are often lack of the history information about the technical and operational threats from people. To evaluate probability of these kind threats, we can use analogy method. However, actually it often depends on analyzers' practical experience. We have proposed a simple method to describe the risk probability in three levels: high, medium, and low. Table 3 shows the definitions of risk probability.

Table 3 Definitions of Risk Probability

Probability	Description
High	Threat source has high motivation and ability, security measures are invalid.
Medium	Threat source has some motivation and ability, but security measure have effect; or threat source does not have motivation; or it does not have obvious ability.
Low	Threat source is lack of motivation and ability, security measures can keep vulnerabilities from attacking effectively.

3.3 Risk Controlling

Risk controlling is to choose and use some risk controlling methods to guarantee the risk can be reduced to an acceptable level. Risk controlling is the most important step in the risk management. It is the key factor to determine whether the risk management is successful or not. The goal of e-government security risk controlling is to reduce the risk degree which e-government projects suffering.

Generally speaking, there are two kinds of risk controlling methods. First are risk controlling measures, such as risk reducing, avoiding, or transferring, and losses managing. We often use risk transferring and losses managing in e-government security risk management.

Second kinds are measures funding for risk compensation, which include insuring, or taking risk by oneself. In e-government security risk management, managers need to decide which measures to choose — insuring or taking risk by their own. In addition, to make a proper choice, one should take risk costs into consideration. Of course, we can not ignore other influences, such as government's reputations.

One effective and feasible risk controlling method for e-government security is establishing a whole security plan to reduce risk, mastering some basic technology for security guarantee, and preparing solutions that the government can adopt when specific security accidents happen. We have designed a process of risk controlling which shown in Figure 1.

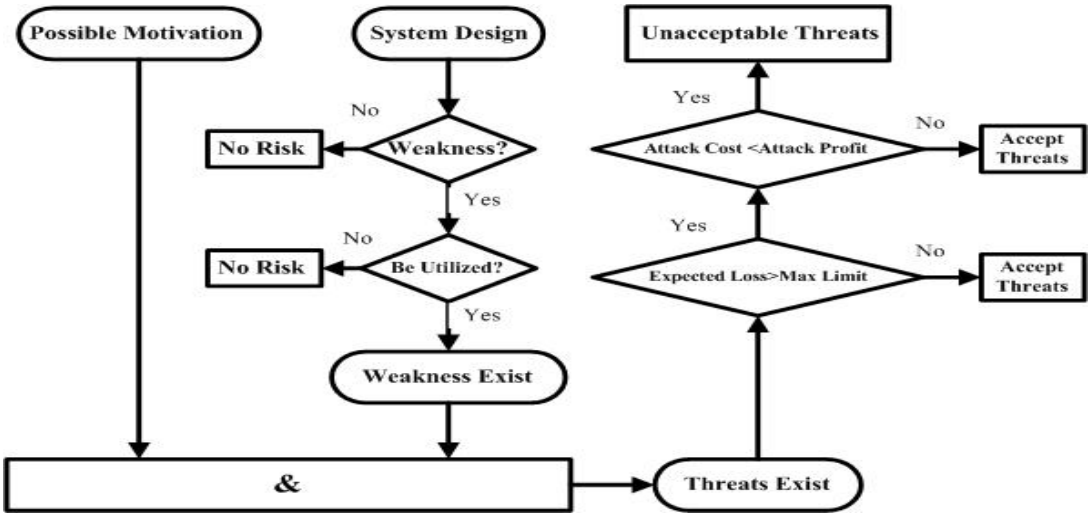

Figure 1 The ess of Risk Controlling

4. Risk Management Countermeasures

Considering the importance of the security of e-government, it is urgent to dispose a whole set of effective countermeasures. The purpose of disposing the countermeasures is to reduce the potential risks and security bugs, so that we can reduce the risk which the e-government system environment facing.

Among the e-government risk management countermeasures, it is popular to use defense-in-depth strategy at present. Defense-in-depth strategy, exactly, is consisted of depth security and multi-level security. Through disposing multi-level security protection, we can guarantee that if one level got broken, other levels can still ensure the security of e-government system resources. For example, in case that the outer firewall of one unit got destroyed, by virtue of the inner firewall, the invader still can not get access to the sensitive data, neither commit any damage to them. Ideally, each level supplies different measures in order to avoid that the hackers can attack different levels in the same way. We have put forward an effective defense-in-defense strategy which is shown in figure 2.

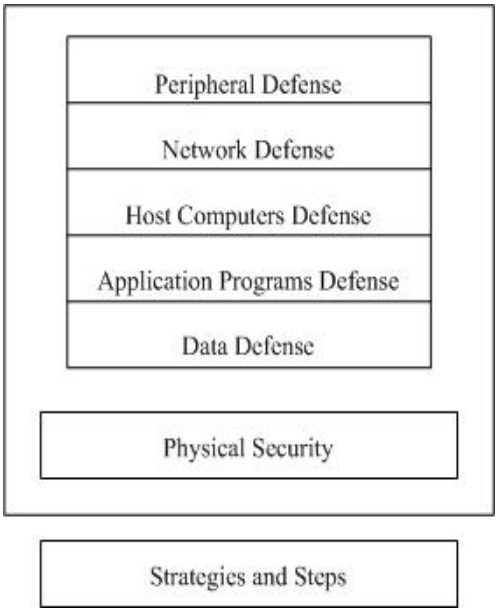

Figure 2 An Effective Defense-in-Depth Strategy

5. Conclusions

Generally speaking, risk management has three basic countermeasures: (1) managers take some proper measures to reduce the probability of risk accidents; (2) managers prepare an emergency plan and adopt it when contingences happen; or (3) managers do nothing.

For already chosen countermeasures, managers should have a full evaluation of their potential risks. And draw up a relevant emergency plan in order to make the possible risk losses minimum.

There are no golden rules for risk management. For e-government security risk management, the first step is to scan and detect internal and external environment of the e-government system, check the vulnerabilities and weaknesses of the system. Patch or append new devices immediately in order to reduce the losses as much as possible while risks happen. Secondly, do a full analysis about the e-government security risk, and then make relevant plans and measures. Track and monitor those plans and measures in each implement stage. At last, adjust risk management measures at any time according to the environment changes, and draw up a whole disaster recovery plan.

Reference

[1] Westerlind K. Evaluating. 2004. Return on Information Technology Investment. School of Economics and Commercial Law. Gothethenburg University.
[2] Theodosios Tsiakis, Stephanides G. 2005. The Economic Approach of Information Security. Computers & Security. No.24. 105-108.
[3] Lawrence A, Gordon, Martin, Ploeb. 2002. The Economics of Information on Security Investment. ACM Transactions on Information and System Security Vol. 5 No. 4. 438-457.
[4] S. Griztalis, C. Lambrinoudakis. 2002. Security Requirements of E-Government Services: an Organizational Framework. Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications. Las Vegas.
[5] Lambrinoudakis, Costas, Griztalis et al. 2003. Security Requirements for E-Government Services: a Methodological Approach for Developing a Common PKI-Based. Security Policy Computer Communications. No.26. 1873-1883.
[6] Leitold H, Hollosi A, Poseh R. 2002. Security Architecture of the Austrian Citizen Card Concept. Computer Security Applications Conference. Proceedings. 18th Annual. 9-13. 391-400.
[7] Wimmer M, Von Bredow B. 2002. A Holistic Approach for Providing Security Solutions in E-Government. System Sciences. HICSS. Proceedings of the 35th Annual Hawaii International Conference. Hawaii: 7-10. 1715-1724.

[8] Conklin A, Whiet G. B. 2006. E-Government and Cyber Security: The Role of Cyber Security Exercises. HICSS' 06. Proceedings of the 39th Annual Hawaii Imitational on System Sciences. Hawai. 79b-79b.
[9] Kun Wang, Lihua Zhou, Zhen Cai, Zengxin Li. 2005. A disaster Recovery System Model in an E-government System. PDCAT 2005. Sixth International Conference on Parallel and Distributed Computing Applications and Technologies. 247-250.
[10] Benabdallah S., Gueniara EI Fatmi S., Oudriga N. B. 2002. Security Issues in E-Government Models: what governments should do? 2002 IEEE International Conference on Systems, Man and Cybernetics. 398-403.
[11] Ji Jianyue, Wang Yuanyue. 2002. On the Subjects of E-government Current Situation, Problems and Development Strategies In Our Country Science of Science and Management of S.& T. Vol. 23. No.6. 14-17. (In Chinese)
[12] Du Wenzhong, Ma Liping. 2005. What Kind of Security Concept E-Government Should Have Network and Computer Security. No.5. 2-4. (In Chinese)
[13] Zhang Weihua. 2005. Some Problems in E-Government Information Security Architecture of Our Country. E-Government. No.8. 10-17. (In Chinese)
[14] Ren Jinhua. 2005. Problems Existing in the E-Government Construction Management in China. E-Government. No.1. P57-72. (In Chinese)
[15] Yan Qiang, Shu Huaying. 2005. Security Risk Management in the E-Government System. Computer Systems & Applications. Vol. 2005 No.10. 2-5. (In Chinese)
[16] Shen Changxiang. 2002. Technical Framework of the System for Safeguarding Electronic Government Information Security. Network Security Technology & Application. No.6. 12-13. (In Chinese)
[17] Wang Huanxi. 2003. E-Government: Risk Analysis and Prevention Strategies The Journal of The Library Science In China. No.5. 49-51. (In Chinese)
[18] Zhang Chongbin, Suo Yanfeng. 2002. The Application of Information Security Technology in E-Government System Netinfo Securit. No.9. 45-46. (In Chinese)