An Approach for Security Management Cost Optimization through Security Value Lifecycle

Sung-Hwan Kim[1], Min-Woo Park[1], Jung-ho Eom[2], and Tai-Myoung Chung[1]

[1] Internet Management Technology Laboratory,
School of Information and Communication Engineering,
Sungkyunkwan University, Chunchun-dong 300,
Jangan-gu, Suwon, Kyunggi-do, Republic of Korea
{shkim47,mwpark}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr
[2] Department of Military Studies, Daejeon University,
62 Daehakro, Dong-Gu, Daejeon-si, 300-716, Republic of Korea
eomhun@gmail.com

Abstract. Security management cost has been increased rapidly, due to development of IT and security issues. In this paper, we focused on the two attributes of information security. The one is the sensitive information (SI) have security value lifecycle. The other is SI that has characteristics to decrease security value over time. We proposed the method that security management cost optimizing using that.

Keywords: Secure Information, Security Management Cost, Security Value Lifecycle.

1 Introduction

The importance of information management cost has increased because of the increased utilization of electronic information, and it is becoming increasingly difficult to ignore security cost. Generally, the information system means the computer environment based electronic data system, and information security means computer system based electronic information security. Electronic information can be stored on a variety of platforms. Thus, there are various types of information security. Sensitive Information (SI) have a high value among information and need to special measure for communication and management. Special measure means the information encryption, access control, policy control and so on. There were many studies that equivalent to the cost of the analysis of the countermeasure cost.

Recent technology developments in information security fields have heightened the need for information security management cost. So far, there has been little discussion about information security value lifecycle. We proposed method to optimize the security management cost using security value lifecycle. This paper has been organized in the following way: we will describe related works in section 2 and our proposed method in section 3 and conclude and future work in the last section.

[2] He is a corresponding author of this paper.

ISA 2013, ASTL Vol. 21, pp. 29 - 32, 2013

2 Related Works

In response to development of information technology, there were many studies on information management cost, information lifecycle and information security.

Bob Blakley et al [1] indicated information security start with policy that describe “who should be allowed to do what” to sensitive information. And then proposed the following four process for enforce the policy; protection measure, detection measure, response measure, assurance measure.

Few studies are limited in that qualitative analysis. Next studies are a quantitative representation of the relationship between security investment costs and the information safety. Bob Blakley et al [1] described the concept of ALE (Annualized Loss Expectation). They propose a method to quantitatively measure a security breach using loss expectation and probability of breach occur.

Theodosios Tsiakis et al [2] approached information security with economic point of view too. They proposed the economic model and describe the economic evaluation method using the ALE, ROSI(Return On Security Investment) and TROI(Total Return On Investment). Also they represented the relation that security investment is proportional security. The study on information lifecycle management (ILM) has been studied since 1990s. ILM was defined as business-centric strategy for proactive management of information via its value [3].

In this paper, we focused on a security attribute of information value. And we propose the optimizing method of total management cost using security value lifecycle while maintaining a security expectation effect.

3 Information Security Value Lifecycle and Total Management Cost Optimization

3.1 Sensitive Information Level and Information Security

SI is commonly expressed as corporate intellectual proprietary or government's secret and so on. The criteria for determining SI depends on the organization’s security policy.

Leaks of SI could give critical damage to public or enterprise. Information leaks mean the steal by external attacker or internal leaks by insider.

In the case of military, SI could be managed by setting the grade according to national security. It is difficult to determine the absolute criteria for Information Security (IS) and task of IS, as discussed in the related woks

We defined IS as activity for information protection from external and internal threats, and we focus on the industrial SI that is given a grading. We classify a four grade to industrial SI depending on the severity of losses on company due to leak.

Table 1. The Level of Sensitive Information

Level	Criteria	Example

I	“Exceptionally huge damage” to enterprise, If it leaks,	· Intellectual property · Patent(Critical technology)
II	“Severe damage” to enterprise, If it leaks,	· New project information · Business strategy
III	“Damage” to enterprise, If it leaks,	· Customer information · Sales information(Detail)
Restricted	“Undesirable effects” to enterprise, If it leaks,	· Human resource information · Business process

Main assumptions are as follows:

- When setting up the initial security level is set to the highest security level that can be granted by applying the most rigorous standards.
- The security level is possible to decrease.
- As the basic unit of management period, month, week, day is available.
- Establish a condition on decrease of security level
- Specify the SI in accordance with the management department
- Security level retention period is adjustable in accordance with the security policy.
- Investment management costs, depending on the security level.

3.2 Security Value Lifecycle

The result of information lifecycle management depends on the standard of value.

In this paper, we selected time and level of SI among the various variable, because of pattern that most Security Level (SL) of SI decrease according to flow of time.

For example, suppose to the new project information of any company. That information has been managed as high security level until project termination. But after that, the security level of the information will decrease to the lower level.

First, we proposed the lifecycle of the SI. Lifecycle of SI has a five stage:

Request for SI → *Create of SI* → *Determine the level of SI* →
Maintain the SI → *Discard of SI*

Second, we set up a four stage Security Level(SL) lifecycle based on lifecycle of SI :

Initial SL → *SL Maintain* → *SL Diminish* → *SL Disappear*

3.3 Total Security Management Cost Model

Lawrence A. Gordon et al [4] described that vulnerability is inversely depending on the level of IS and information security is proportional to security investment. They explained that optimal value of security investment. The optimal value could be said to a ceiling point that there is no security effect increase.

In view of that, we designed total security management cost model for finding an optimal cost.

- Parameter declarations:

File Management Cost of Level i	: MC(i)
Total Security Management Cost of file X	: TSMC(X)
Management Period of Level i	: MP(i)

Assuming that any SI, X1. The total security management cost of SP is as follows:

$$TSMC(X1) = MC(1) \times MP(1) + MC(2) \times MP(2) + MC(3) \times MP(3) + MC(RI) \times MP(RI) \tag{1}$$

It is a key point of total security management cost optimization by investment depending on security level (value), not to apply the same security level for the entire period.

4 Conclusion and Future Work

We set up the information security lifecycle, and proposed method to optimize the total security management cost using that. We focused on character of SI that security value decrease over time. Continue to increase the scale of the digital information grows exponentially, the quantity of the SI that must be protected than ever before.

In the future, we will study on the automatic control for information security value. Also, we plan to study the proposed method in this paper how to apply Big Data.

5 Acknowledgements

We work was supported by the IT R&D program of MKE/KEIT. [10041244, Smart TV 2.0 Software Platform]

References

1. Blakley, B., McDermott, E., Geer, D.: Information Security is Information Risk Management. (2001) 97-104
2. Tsiakis, T., & Stephanides, G.: The Economic Approach of Information Security. Comput. Secur., 24 (2005) 105-108
3. Reiner, D., Press, G., Lenaghan, M. et al.: Information Lifecycle Management: The EMC Perspective. (2004) 804-807
4. Gordon, L. A., & Loeb, M. P.: The Economics of Information Security Investment. ACM Transactions on Information and System Security (TISSEC), 5 (2002) 438-457