The Methodology of Security Management Cost Reduction using Security Level Lifecycle

Sung-Hwan Kim[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
[2] Department of Military Studies, Daejeon University,
62 Daehakro, Dong-Gu, Daejeon-si, 300-716, Republic of Korea
[1]shkim47@imtl.skku.ac.kr, [2]eomhun@gmail.com
[1]tmchung@ece.skku.ac.kr

Abstract

Security management cost for securing information is increasing rapidly, as increasing the use of electronic information. In this paper, we focused on the two respects. The one is security level lifecycle of the sensitive information (SI). The other is SI that has characteristics to decrease security level over time. We proposed the method that total security management cost reducing than before applying by differential costing over security level lifecycle. Also, we considered of predictability on security level decrease together. Last, we expressed the cost reduction target area through a comparison of the cost model.

Keywords: *Information security, Sensitive information, Security management cost, Security level lifecycle, Security management cost model, Cost reduction area*

1. Introduction

The importance of information management cost has increased due to the increased utilization of electronic information, and it is becoming increasingly difficult to ignore security cost for secure information. In general, 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 a little discussion about information security level 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. We explain the case study of proposed method in Section 4 and conclude and future work in the last section.

[*] He is corresponding author of this paper.

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.

In the research report [2], Mikko T. Siponen, *et al.*, identified four security issues; access to information systems, secure communication, security management, development of secure information system.

As can be seen from several related studies we've seen so far, information security is a series of activities to protect and to ensure the information and enforce the reliability and validity of the information from the abnormal behavior of the external or internal.

However, 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 proposed a method to quantitatively measure a security breach using loss expectation and probability of breach occur.

Theodosios Tsiakis, *et al.*, [3] 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 [5]. Author emphasizes the need for proper classification of value and information management.

Gerhard Fischer, *et al.*, [4] classified ILM to the four main stages (Send time, Read time, Question time and Storage time). And then they proposed the situation and system model for relationship between issue and action.

Ying Chen [6] divided task of ILM into three group; information valuation, information characterization & classification and Task prioritization & optimization. And he proposed the information valuation modeling.

Ray Bernad [7] proposed the method for information lifecycle security risk assessment. Also he describes the information lifecycle security risk assessment.

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

3. Information Security Level Lifecycle and Total Security 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 to restricted level at a time.
- 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.
  - Management cost: Related to Encryption, Storage, Communication, Authentication, *etc*.

In the next section, we will propose the total management cost optimization method with assumed industrial SI.

3.2. Security Level Lifecycle

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

In case of [6], Usage and time have been used in the valuation model.

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 sensitive information. Lifecycle of SI has a five stage, as follow:

$$\textit{Request for SI} \rightarrow \textit{Create of SI} \rightarrow \textit{Determine the level of SI} \rightarrow$$
$$\textit{Maintain the SI} \rightarrow \textit{Discard of SI}$$

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

$$\textit{Initial SL} \rightarrow \textit{SL Maintain} \rightarrow \textit{SL Diminish} \rightarrow \textit{SL Disappear}$$

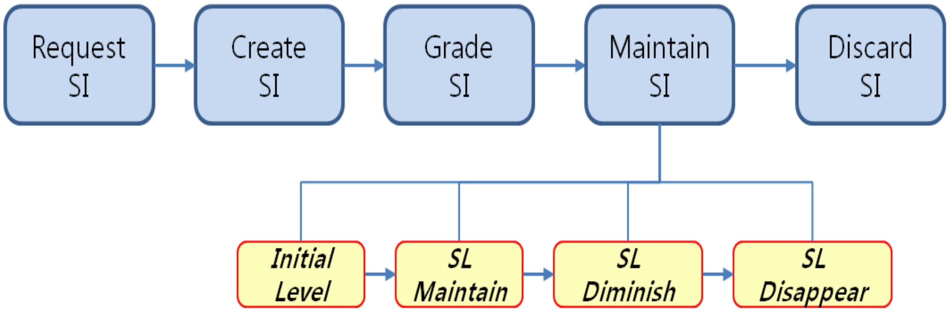

Figure 1. Lifecycle of SI and Lifecycle of SV

3.3. Total Security Management Cost Model

Lawrence A. Gordon, *et al.*, [8] 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. We considered two cases. First, Security lifecycle of SI was predictable. Second, it was unpredictable.

If the prediction of the change of state, the security management cost estimation model is as follows.

- Parameter declarations:

- Current Level of SI : k

- Management Cost of level k in unit management period : MC(k)

  * MC(RI) < MC(III) < MC(II) < MC(I)

- Total number of Management Period of SI on level k : MP(k)

- Total number of cost estimation unit period of SI : N

- Total Security Management Cost of SI during N period : TSMC(SI_N)

The total security management cost of SI_N can be written as:

$$TSMC(SI_N) = MC(I) \times MP(I) + MC(II) \times MP(II) + MC(III) \times MP(III) + MC(RI) \times MP(RI) \qquad \textbf{(1)}$$

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.

Next, state transition of security level was unpredictable case. As previous assumptions, security level could not increase.

Let P_1, P_2, P_3 are random variable that the probability of a downgrade and one line expressed the one unit period. State transition of security level and state transition probability of each SL can be expressed as the following figure and table.

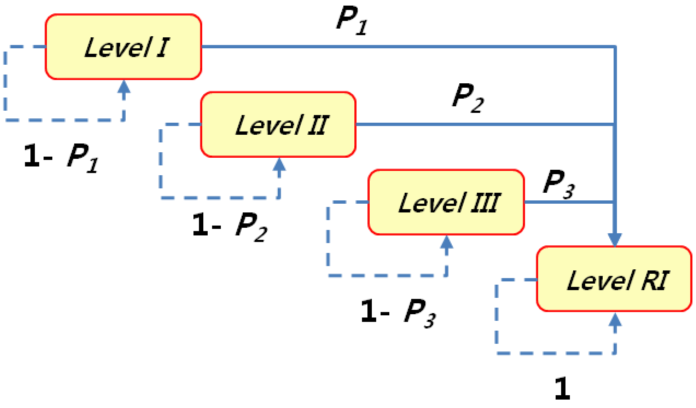

Figure 2. State Transition Diagram of Security Level

Next, we considered that state transition of security level was unpredictable case. As previous assumptions, security level could not increase. Following figure depicts the possible state of security level over management period.

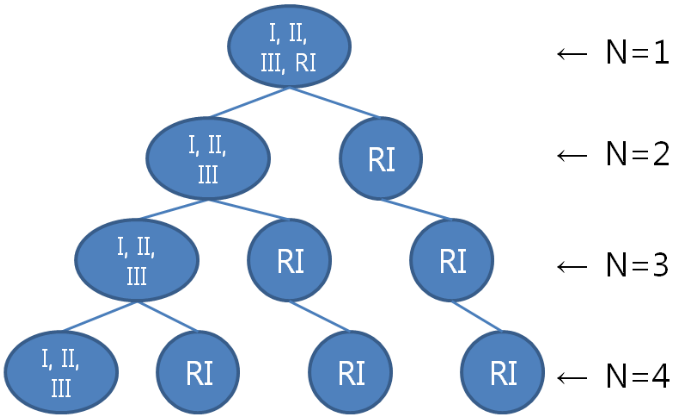

Figure 3. State Transition Tree of Security Level (N=1~4)

As you can see from the Figure 3, total security management cost distribution depend on the Initial SL and N.

Accordingly, let P_k be a probability of downgrade from level k to level RI.(P_{RI} is 1)

Security Management Cost(SMC) in ***n***th period can be rewritten as: SI_i

- $n = 1$, $SMC(SI_n)=MC(k$

- $n = 2$, $SMC(SI_n)=MC(k)(1-P_k) + MC(RI)(P_k)$
- $n \geq 3$, $SMC(SI_n) = (1-P_k)^{n-1} \times MC(k) + P_k\{1+\ldots + (1-P_k)^{n-2}\}\times MC(RI)$

Therefore,

$$TSMC(SI_N) = \sum_{i=1}^{N} SMC(SI_i) \qquad \textbf{(2)}$$

- *If initial level is RI, then*

$$TSMC(SI_N) = N \times MC(RI) \qquad \textbf{(3)}$$

In the next section, we explain the improving of proposed model through the case study.

4. Case Study

In this section, we try to demonstrate the improvement of our proposed method by following examples. Firstly, we assumed that virtual company "a" and its department 'b'.

Let department 'B' have many kinds of SI as follow:

Table 2. Current status of SI in the department B

Security Level	Management Cost per month($)	Total Number of Possession (ea)
I	50	1
II	40	1
III	30	1
RI	10	1

Also, monthly change of SI security level in department B is as follow:

Table 3. Monthly Security Level (Department B)

No	Main Content of SI	Initial Level of SI	**Monthly Security Level of SI**											
			1	2	3	4	5	6	7	8	9	10	11	12
1	Intellectual property	I	I											
SL comment			SL is valid											
2	Summer Season Sales strategy	II	II								RI			
SL comment			SL valid								Season off			
3	The first quarter Sales Information	III	III			RI								
SL comment			SL is valid			Expiration of the term								
4	Department Business Process	RI	RI											
SL comment			SL is valid											

Secondly, we estimated the annual TSMC in common method. Common method means that ignoring the security value lifecycle. So, annual security management cost in department 'B'[TSMC(Common_B$_{12}$)] can be calculated by substituting in Formula 1 as follows:

$$TSMC(Common\_B_{12}) = \{MC(I) + MC(II) + MC(III)+MC(RI)\} \times 12 = 1560(\$)$$

Next, we estimated the TSMC using proposed method. If we could predict the decrease of security value, annual security management cost[TSMC(Pro_predict_B$_{12}$)] was as follows:

Where $MP(I) = 12$, $MP(II) = 8$, $MP(III) = 3$, $MP(RI) = 25$

Therefore,

$$TSMC\ (Pro\_predict\_B_{12}) = MC(I) \times MP(I) + MC(II) \times MP(II) + MC(III) \times MP(III) + MC(RI) \times MP(RI) = 1260(\$)$$

Finally, In case of unpredictable case, TSMC(Pro_unpredict_B$_{12}$) can be calculated by substituting in Formula 2 and 3 as follows:

Where $N=12$, *Initial Level No.1/ No.2/ No. : Level I/ II/ III, Initial Level of No. 4 is RI,*
$P_I = 0.02$, $P_{II} = 0.03$, $P_{III} = 0.05$

$$TSMC(Pro\_unpredict\_B_{12}) = TSMC(Pro\_unpredict\_No.\ 1_{12}) + TSMC(Pro\_unpredict\_\ No.\ 2_{12}) + TSMC(Pro\_unpredict\_\ No.\ 3_{12}) + TSMC(Pro\_unpredict\_\ No.\ 4_{12})$$

Therefore,

$$TSMC(Pro\_unpredict\_B_{12}) = \sum_{i=1}^{12} SMC\,(No.1_i) + \sum_{i=1}^{12} SMC\,(No.2_i) + \sum_{i=1}^{12} SMC\,(No.3_i) + 12 \times MC(RI) = 553.7 + 426.1+303.4+120$$

$$= 1403.2(\$)$$

This implies that, $TSMC(Pro\_predict) < TSMC(Pro\_unpredic) < TSMC(Common)$

So far, it is clear that proposed method could reduce the total security management cost.

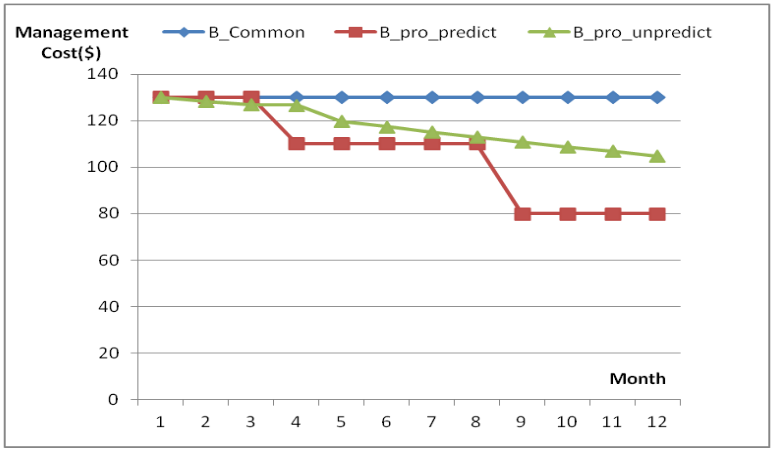

Figure 4. Total Security Management Cost as a Model

We compared the two results by increasing the P_i(P2) as shown in the following figure for confirming the correlation between probability and security management cost.

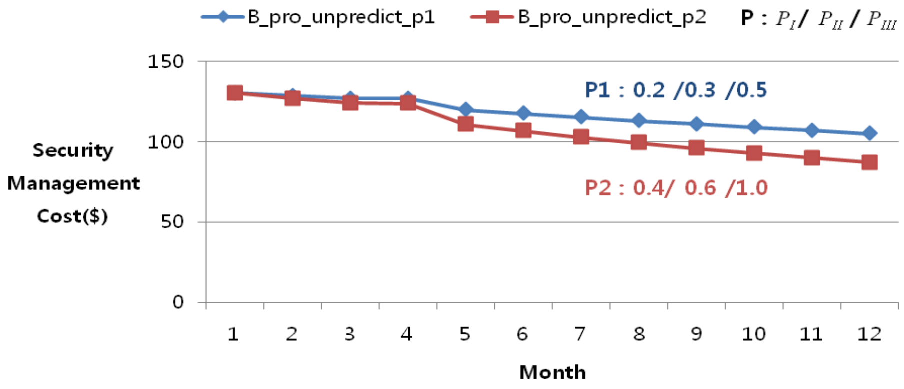

Figure 5. Correlation between P_i and Total Management Cost

Figure 5 implies that security cost reduction increase depending on P_i. To this end, security level lifecycle including security level decrease became an important issue.

As you can see the below Figure 6, the total security management cost can be expressed as the area of the plane.

Reduction in available area of the total security management cost was expressed as cost reduction target area. Thus, cost savings can be expressed as the difference between B_Common and B_Pro_unpredict applying the proposed method. As described so far, Cost reduction range depending on the downgrade probability and initial security level of SI. At this point, key contribution of this paper proposed a method to identify and increase reduction cost.

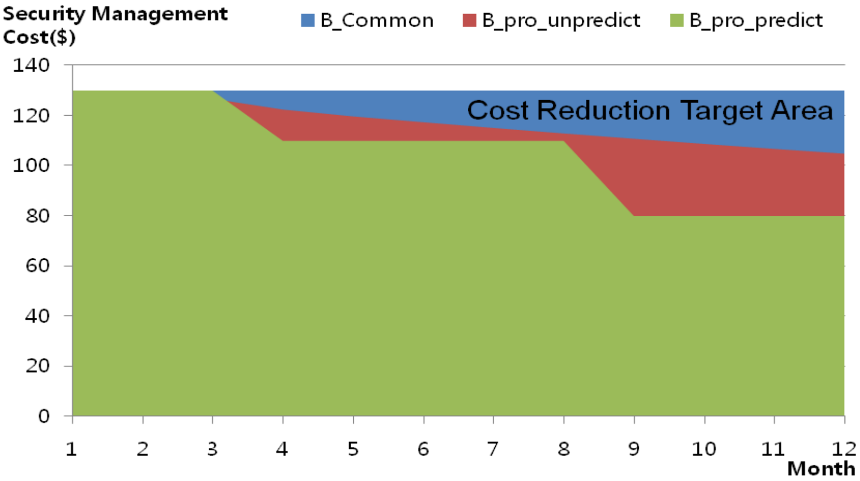

Figure 6. Security Management Cost Reduction Target Area

5. Conclusion and Future Work

We set up the information security lifecycle, and proposed method to reduce the total security management cost using that. We focused on character of SI that security level decrease over time. Also we considered that predictability of security level downgrade. The key aspect of our proposed method is that total security management cost reduction by differential investment depending on security level.

Continue to increase the scale of the digital information grows exponentially, the quantity of the SI that must be protected than ever before. So, in the future, we will study on the automatic monitoring for information security value. Also, we plan to study the proposed method in this paper how to apply Big Data.

Acknowledgements

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

References

[1] B. Blakley, E. McDermott and D. Geer, “Information Security is Information Risk Management, **(2001)**, pp. 97-104.

[2] M. T. Siponen and H. Oinas-Kukkonen, “A Review of Information Security Issues and Respective Research Contributions”, ACM Sigmis Database, vol. 38, **(2007)**, pp. 60-80.

[3] T. Tsiakis and G. Stephanides, “The Economic Approach of Information Security”, Computer Security, vol. 24, **(2005)**, pp. 105-108.

[4] G. Fischer and C. Stevens, “Information Access in Complex”, Poorly Structured Information Spaces, **(1991)**, pp. 63-70.

[5] D. Reiner, G. Press and M. Lenaghan, “Information Lifecycle Management”, The EMC Perspective, **(2004)**, pp. 804-807.

[6] Y. Chen, “Information Valuation for Information Lifecycle Management”, **(2005)**, pp. 135-146.

[7] R. Bernard, “Information Lifecycle Security Risk Assessment: A Tool for Closing Security Gaps”, Computer. Security, vol. 26, **(2007)**, pp. 26-30.

[8] L. A. Gordon and M. P. Loeb, “The Economics of Information Security Investment”, ACM Transactions on Information and System Security (TISSEC), vol. 5, **(2002)**, pp. 438-457.

[9] S. -H. Kim, M. -W. Park, J. -H. Eom and T. -M. Chung, “An Approach for Security Management Cost Optimization through Security Value Lifecycle”, Proceedings of the 7th International Conference on Information Security and Assurance, Cebu, Philippines, **(2013)** April 26-28.

Authors

Sung hwan Kim received the M.S degree in Computer ScienceEngineering from Seoul National University, Seoul, Korea, in 2006. He is currently working toward the Ph.D. degree in the School of Information & Communication Engineering, Sungkyunkwan University, Suwon, Korea. His research interests are Information Security, Cyber warfare and SCADA Security.

Jung ho Eom received his M.S. and Ph.D. degrees in Computer Engineering from Sungkyunkwan University, Suwon, Korea in 2003 and 2008, respectively. He is currently a professor of Military Studies at Daejeon University, Daejeon, Korea. His research interests are information security, cyber warfare, network security.

Tai myoung Chung received his first B.S. degree in Electrical Engineering from Yonsei University, Korea in 1981 and his second B.S. degree in Computer Science from University of Illinois, Chicago, USA in 1984. He received his M.S. degree in Computer Engineering from University of Illinois 1987 and his Ph.D. degree in Computer Engineering from Purdue University, W. Lafayette, USA in 1995. He is currently a professor of Information and Communications Engineering at Sungkyunkwan University, Suwon, Korea. He is now a vice-chair of the Working Party on Information Security & Privacy, OECD.