A security measure selection scheme with consideration of potential lawsuits

Takumi Yamamoto[1], Yuma Usui[2], Fumihiko Magata[3], Yoshimi Teshigawara[4],
Ryoichi Sasaki[5], Masakatsu Nishigaki[1,6]
[1]Graduate School of Science and Technology, Shizuoka University, 3-5-1, Johoku, Naka, Hamamatsu, Japan
[2]Graduate School of Informatics, Shizuoka University, 3-5-1, Johoku, Naka, Hamamatsu, Japan
[3]NTT Information Sharing Platform Laboratories, 3-9-11 Midori-Cho, Musashino-Shi, Tokyo, 180-8585 Japan
[4]Graduate School of Engineering, Soka University, Tangimachi, Hachioji, Tokyo 192-8577 Japan
[5]Graduate School of Science and Technology, Tokyo Denki University, 2-2 Kanda-Nishiki-Cho, Chiyoda-Ku,
Tokyo 101-8457 Japan
[6]Japan Science Technology and Agency, CREST
E-mail: nisigaki@inf.shizuoka.ac.jp

Abstract - *Information breaches on ITC systems may result in lawsuits. Information security countermeasures such as firewalls, data encryption, and so on, are essential; protecting systems against security threats including viruses and hackers reduces the likelihood of incidents such as information leakage due to illegal access and service suspension due to denial-of-service attacks. However, there are no perfect countermeasures. Therefore, companies and organizations must be prepared for litigation. That is, digital forensic countermeasures (management of a variety of system event logs) should be considered an important part of an information security strategy. An approach is described for formulating an optimization problem to select both security and forensics countermeasures that maximize cost-effectiveness.*

Keywords: information security management system, digital forensics, countermeasure selection, lawsuit

1 Introduction

Ensuring security for information technology and communication (ITC) systems is essential for most companies and organizations. Frequent information leakage incidents have inspired organizations to take seriously the need to protect their information. Therefore, many organizations have introduced security management policies using information security management systems (ISMS). The development of ISMS methods and tools has become an active area of research [1][2].

However, there is still no end to security incidents. According to an investigation of the Japan Security Network Association (JNSA), the number of cases of individual information leakage incidents and accidents in 2008 was a record high of 1,373 times in Japan [3]. In America, more than 41 million credit and debit card numbers were stolen by cracking. The criminals drove around and scanned the wireless networks of retailers to find security holes in a practice known as “war driving.” Once the criminals identified technical weaknesses in the networks, they installed sniffer programs from collaborators overseas [4].

Recovering from a security incident usually takes time and money. At worst, it may result in lawsuits. In Japan, there have been two famous cases. One was a leakage of customer information by Yahoo!BB that exposed the personal information of 4.5 million customers. SoftBank, the managing company of Yahoo!BB, sent cash vouchers for 500 yen to all customers as an apology. But, the company was the target of a class action lawsuit and was ordered to pay approximately 5,500 yen in damages to each of five plaintiffs [5]. The other case was a leakage of customer information from TBC group that exposed personal data of fifty thousand customers. The company was the target of a class action lawsuit and was ordered to pay approximately 35,500 yen in damages to each of thirteen plaintiffs [6].

In a worst-case scenario, if all 4.5 million plaintiffs brought a suit and the defendant were ordered to pay 35,500 yen to each, the defendant would have to pay a huge indemnity.

Also, the indemnity caused by the leak of a product blueprint or of proprietary technical information could be huge. Additionally, if an organization’s ITC resources were used by an unauthorized person to wreak havoc on other systems, the organization could get sued.

As in the examples given above, dissatisfied victims may sue the entity who caused the damage. Therefore, organizations have to address not only direct damage caused by security incidents, but also the indirect damage of litigation resulting from the incidents.

However, the existing methods and tools of ISMS mostly minimize only the direct damage from incidents occurring. Thus, this study tries to show a method of selecting the best combination of countermeasures considering litigation and compensation for damage (indirect damage) due to security incidents or accidents.

If there are no security incidents, there will be no litigation claims. Therefore, first and foremost, organizations should adequately deploy existing security countermeasures based on ISMS (e.g., firewalls and data encryption). However, in the real world, absolute countermeasures do not exist. Therefore, it is necessary to combine digital forensic countermeasures (management of a variety of system event logs) with existing information security countermeasures. We describe an approach to formulating an optimization problem for selecting both security countermeasures and forensic countermeasures while considering cost efficiency.

2 Method

2.1 ISMS countermeasures

We define "ISMS countermeasures" as measures to prevent security incidents and accidents. This includes all existing information security methods and tools, such as firewalls, data encryption, and access control [1].

Appropriate ISMS countermeasures can reduce the possibility of security incidents and help organizations can prevent loss of assets (direct damage) caused by security incidents and decrease indirect damage by preventing lawsuits.

Selecting ISMS countermeasures begins with risk analysis: sorting out information assets and calculating their value and sorting out threats and estimating the probability of incidents that could be caused by the threats. By multiplying the value of assets by the probability of incidents, the expected value of loss (EVL) is calculated. Thus, EVL is expressed as

$$EVL = \sum_{k} VA_k PI_k \quad , \qquad (1)$$

where VA_k is the value of the k-th asset and PI_k is the possibility of incidents that can affect the k-th asset (Fig. 1).

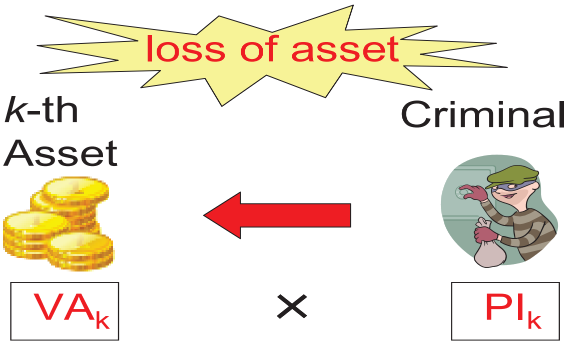

Figure 1 EVL: Expected Value of Loss

Following the risk analysis, impact analysis of countermeasures is carried out: sorting out every possible security countermeasures against the threats identified in the risk analysis and examining how much the countermeasures can reduce the probability of incident occurrence.

The best available countermeasures should be chosen so that the highest effect can be obtained with the least expense. Thus, selecting ISMS countermeasures is formulated as

$$Min(EVL \cdot E_{ISMS} + C_{ISMS}) \qquad (2)$$

where EVL is the expected value of loss, E_{ISMS} is how much the selected ISMS countermeasures can reduce the probability of incident occurrence, and C_{ISMS} is the cost of the selected countermeasures (Fig. 2).

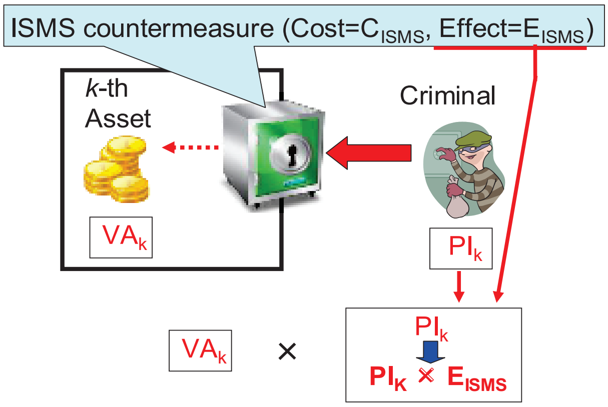

Figure 2 EVL with ISMS countermeasure

2.2 DF countermeasures

We define "digital forensic (DF) countermeasures" as countermeasures to reduce compensation for damage (indirect damage) when security incidents or accidents go into litigation. DF countermeasures are mainly techniques that conserve and manage system event logs and user operation logs.

There are two good reasons for the use of DF countermeasures. First, if an organization suffers damage from a criminal (including an insider), the DF countermeasures can aid in investigating and building legal case against the criminal to sue for damages. Second, if an organization is sued for a security incident, the DF countermeasures can help to show legal evidence of the scope and the degree of the organization's negligence.

Selecting DF countermeasures begins with lawsuit risk analysis: sorting out potential lawsuits and estimating the value of compensation, the probability of litigation and the possibility of losing the cases. By multiplying the value of compensation, the probability of the litigation, and the probability of losing, the expected value of compensation (EVC) is calculated.

Basically, victims go to court to seek compensation for damages suffered from the loss of assets. Therefore, to calculate EVC, we evaluate compensation on an asset-by-asset basis and sum all the potential compensation. Let I_k be defined as an incident that can affect the k-th asset, and L_k be defined as litigation caused by I_k. Then, EVC is expressed as

$$EVC = \sum_k VC_k PO_k PL_k \qquad (3)$$

where VC_k is the value of the compensation caused by L_k, PO_k is the possibility of L_k, and PL_k is the possibility of losing L_k (Fig. 3)..

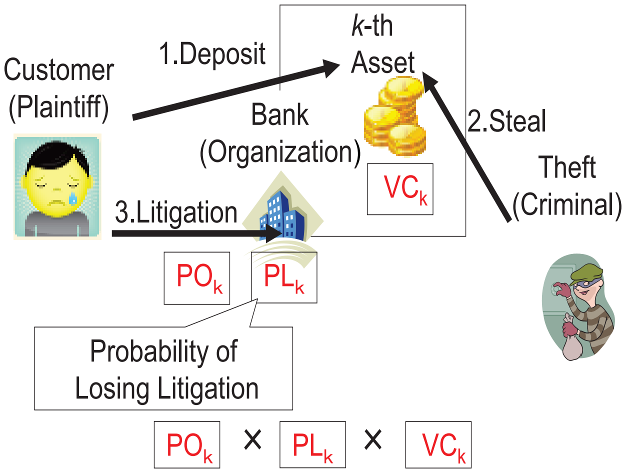

Figure 3 EVC: Expected Value of Compensation

It is noted that DF countermeasures are not yet considered in this lawsuit risk analysis phase. In this paper, we assume that if no DF countermeasures are used, the organization always loses the case. That is, PL_k in Eq. (3) can be set as 1.0. Thus, Eq. (3) is simplified as

$$EVC = \sum_k VC_k PO_k \qquad (4)$$

Following the risk analysis, the impact analysis of countermeasures is carried out: sorting out every possible forensic countermeasure against the litigation identified in the risk analysis and examining how much the countermeasures can reduce the probability of losing the cases.

The best available countermeasures should be chosen so that better outcomes can be obtained at less expense. Thus, the selected DF countermeasures are formulated as

$$Min(EVC \cdot E_{DF} + C_{DF}) \qquad (5)$$

where EVC is the expected value of compensation, E_{DF} is how much the selected DF countermeasures can reduce the probability of losing the cases, and C_{DF} is the cost of the selected countermeasures (Fig. 4).

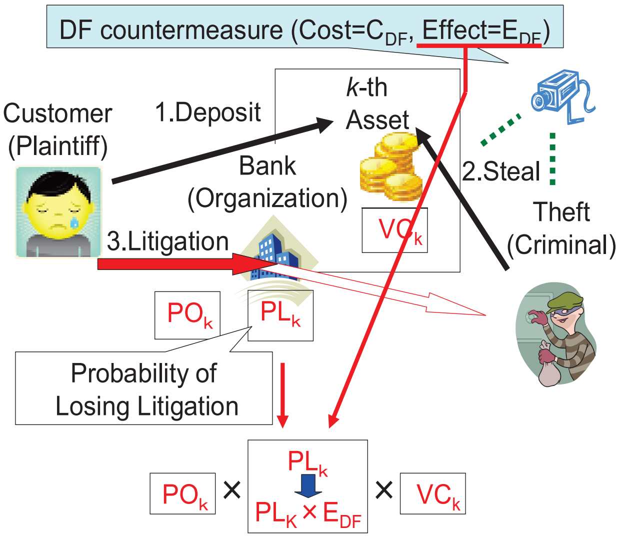

Figure 4 EVC with DF countermeasure

2.3 Selecting the best combination of ISMS and DF countermeasures

With the use of Eqs. (1) to (5), the selection of both ISMS and DF countermeasures is formulated as

$$Min(Loss + Cost) \quad (6)$$

$$Loss = EVL \cdot E_{ISMS} + EVC \cdot E_{DF} =$$

$$(\sum_k VA_k PI_k)E_{ISMS} + (\sum_k VC_k PO_k)E_{DF} \quad (7)$$

$$Cost = C_{ISMS} + C_{DF} \quad (8)$$

Suppose that a set of ISMS countermeasures is applied to an ITC system. Then, how is the effect of countermeasures (E_{ISMS}) evaluated? Security threats differ from asset to asset, and the countermeasures differ from threat to threat. This means that the effect of the applied ISMS countermeasures differs from asset to asset. Therefore we evaluate E_{ISMS} on an asset-by-asset basis. Let I_k be defined as an incident that can affect the k-th asset, and EI_k be defined as the effect of the applied ISMS countermeasures to each I_k. Thus we obtain

$$(\sum_k VA_k PI_k)E_{ISMS} = \sum_k VA_k PI_k EI_k \quad (9)$$

In a similar way, litigation differs depending on which asset is lost, and the countermeasures differ from litigation to litigation. So, the effect of the applied DF countermeasures (E_{DF}) differs from asset to asset. Therefore we evaluate E_{DF} on an asset-by-asset basis, too. Again, let I_k be defined as an incident that can affect the k-th asset and L_k be defined as litigation caused by I_k. Then, by letting EL_k be defined as the effect of the applied DF countermeasures to each L_k, we obtain

$$(\sum_k VC_k PO_k)E_{DF} = \sum_k VC_k PO_k EL_k$$

(10)

The possibility of incidents and of litigation has a subservient relationship because lawsuits are filed when security incidents that affect assets occur. That is, incident I_k (the loss of the k-th asset) will cause litigation L_k. So, we obtain

$$PO_k = \alpha PI_k EI_k \quad (11)$$

where is the frequency rate at which an incident escalates to litigation.

With the use of Eqs. (9) to (11), Eq.(7) is expressed as follows.

$$Loss = \sum_k PI_k EI_k (VA_k + \alpha VC_k EL_k)$$

(12)

Then, Eqs. (6), (8), and (12) are formulas for selecting the best combination of both ISMS and DF countermeasures.

3 Conclusions

We described an approach to formulating an optimization problem that maximizes cost-effectiveness in the selection of both information security and digital forensics countermeasures. In the future, we will evaluate our method by using it to solve several concrete examples.

Acknowledgements

This research was partially founded by Secom Science and Technology Foundation grant.

References

[1] Gordon, L.A. and Loeb, M.P.: The Economics of Information Security Investment, ACM Trans. Information and System Security, Vol.5, No.4, pp.438-457 (2002).

[2] Itsukazu Nakamura, Toshiyuki Hyodo, Masakazu Soga, Tadanori Mizuno, Masakatsu Nishigaki: Practical Approach for Security Measure Selection Problem And Its Availability, IPSJ (Information Processing Society of Japan) Journal, Vol.45, No.8, pp.2022-2033 (2004). (in Japanese)

[3] JNSA: Survey Report of Information Security Incident 2008, http://www.jnsa.org/result/2008/surv/incident/2008incidentsurvey_v1.1.pdf. (in Japanese)

[4] The New York Times: 11 Charged in Theft of 41 Million Card Numbers, http://www.nytimes.com/2008/08/06/business/06theft.html?_r=1

[5] The Japan Times ONLINE: Theft costs Yahoo BB provider little, http://search.japantimes.co.jp/cgi-bin/nn20060520b1.html

[6] The Japan Times ONLINE: Beauty chain ordered to pay damages for loss of personal info., http://search.japantimes.co.jp/cgi-bin/nn20070209a7.html