ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

# 이 기종의 보안 솔루션 통합 운영을 위한 최적의 보안 투자 결정 모델☆

# A Framework for Making Decision on Optimal Security Investment to the Proactive and Reactive Security Solutions management

최 윤 호[1*]
Yoon-Ho Choi

**요 약**

IT 보안의 중요성으로 인해 IT 보안 솔루션의 성능 및 기업의 보안에 대한 투자는 꾸준히 증가하고 있지만, 보안 사고 발생으로 인한 기업의 금전적 손실 감소는 여전히 기대에 미치지 못하고 있는 상황이다. 보안 솔루션을 운영하고 있는 기업을 상대로 한 조사 결과에 따르면, 기업의 보안 솔루션에 대한 이해 부족과 잘못된 투자 전략이 기업의 투자 대비 보안 효율성 향상을 기대에 미치지 못하게 하는 주요한 원인으로 분석되었다. 본 논문에서는 기업의 보안 솔루션에 대한 잘못된 투자로 인한 투자 대비 보안 효율성 저하 문제를 해결하기 위한 보안 투자 결정 모델을 제안한다. 구체적으로는, IT 자산의 취약성 이용 공격으로 인한 조직의 피해 발생 이전에 보안 사고 예방이 가능한 사전 보안 솔루션(Proactive Security Solutions, PSSs)과 조직의 피해 발생 이후에 보안 사고를 조사 및 분석할 수 있는 사후 보안 솔루션 (Reactive Security Solutions, PSSs)에 대한 기업의 투자 방법론을 결정하기 위한 포괄적인 수학적 모델을 제안한다. 또한, 제안된 분석 모델을 사용하여 보안 솔루션의 다양한 매개 변수 영향력 아래에서 조직의 IT 보안 투자 예상 순 이익(expected net benefit)을 극대화하기 위한 최적의 방안을 모색한다.

☞ 주제어 : 의사 결정, 수학적 분석, 보안 솔루션 투자, 최적의 보안 투자

**ABSTRACT**

While IT security investment of organizations has been increased, the amount of the monetary loss of organizations caused by IT security breaches did not decrease as much as their expectation. Also, from surveys, it was discovered that the poor usage of their security budget thwarted the improvement of the organization's security level. In this paper, to resolve the poor usage of security budget of organizations, we propose a comprehensive economic model for determining the optimal amount of investment in security solutions, including the proactive security solutions(PSSs) and the reactive security solutions(RSSs). Using the proposed analytical model under different parameters of security solutions, we show the optimal condition to maximize the expected net benefits from IT security investment of organizations. Also, we verify the common belief that the optimal level of investment in security solutions is an increasing function of vulnerability. Through simulations, we find the optimal level of IT security investment, given parameters of different characteristics of security solutions.

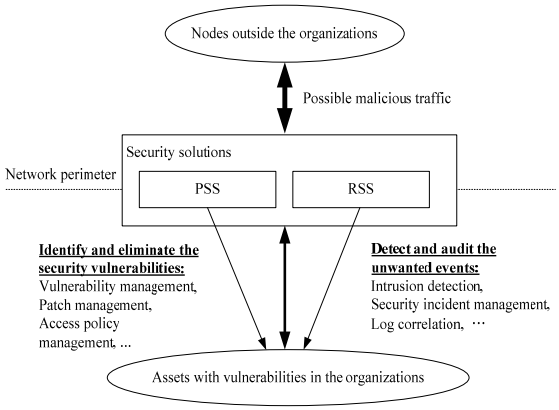
☞ keyword : decision making, mathematical analysis, investment on security solutions, optimal security investment

## 1. INTRODUCTION

From the survey of CSI/FBI [1], the ratio of organizations allocating more than five percent of their IT budget to security investment has increased from 27 percent in 2005 to 34 percent in 2006. However, in spite of a significant amount of monetary investment to improve the security level of organizations, 2012 McAfee threats report shows the increase of IT security breaches in the last four years[2]. Here, the term 'security level' represents the degree to which an organization can control the security flaws in the organization's IT assets such as hardware or software. Also, in [1], it was discovered that the poor decision making process on IT security investment thwarted the improvement

[1] Department Of Convergence Security, Kyonggi University, Suwon, Kyeonggi-do, 443-760, Korea.
[*] Corresponding author (ychoi@kyonggi.ac.kr)
[Received 22 January 2014, Reviewed 25 January 2014(R2 24 March 2014), Accepted 08 April 2014]
☆ 본 연구는 한국연구재단 논문연구과제(NRF-2013R1A1A1005991) 지원으로 수행되었습니다.

of the organization's security level.




(Figure 1) Abstract models for the integrated security solution, where the line width indicates the amount of malicious traffic

In general, organizations decide on investment in security by following a decision process. After determining the assets that need to be protected, organizations investigate the capability of the security solutions, including the proactive security solutions(PSSs) and the reactive security solutions (RSSs). As shown in Figure 1, while PSSs protect the attests by identifying and eliminating their vulnerabilities, the RSSs protect the attests by detecting and auditing the unwanted events which exploit the vulnerabilities. When the capability of the security solutions is quantified and the cost function is given, they select the available solutions that satisfy the optimal level of investment. Thus, the organization can minimize the likelihood that security incidents occur through the given investment.

To evaluate the effectiveness of IT security investment, many analytical approaches have been introduced [3]-[12]. Among them, the traditional risk or decision analysis approach [6]-[12] is known to be a useful method of deciding which solution should be deployed or how much to invest. The idea behind this approach is to identify the potential risks caused by the attacks, the expected loss and their likelihoods, which are used to compute the monetary loss. However, most of the decision analysis approaches treat security solutions as a black box. Thus, they do not determine how the different parameters of security solutions affect the overall security level of the organization and its investment.

To resolve the above problem, Cavusoglu et al. [11] offered a comprehensive analytical model to evaluate IT security investment decisions using the game theory. Cavusoglu et al. determined probability of intrusion in the presence and absence of alerts using the Bayes' rule. However, this model cannot be used to determine how the PSSs and RSSs can substitute or complement each other. This is because the different decision variables have different improvement results and thus, the model does not provide any insights for the capability of the integrated security solution whose performance is measured from the non-overlapped combination of the different characteristics of decision variables. To overcome the limitation, we propose a new analytical model based on the unified model that takes into account all of the decision variables from an information-theoretic viewpoint [13]. Note that a cost-benefit analysis is useful for budgeting information security expenditures [14, 15]. In this paper, based on the expected net benefit as a useful cost-benefit analysis and an information-theoretic performance analysis model, we propose a comprehensive economic model that can determine the optimal amount of investment in the integrated security solution given values of the input and output parameters.

The main contributions of this work can be summarized as follows: (1) We propose an economic model that extends the characteristics of conceptual optimality given by Rowe and Gallaher [10] for the first time. The proposed economic model specifically address how capability of the integrated security solution affects the optimal amount of investment that should be devoted to securing the IT assets. Thus, (2) we find the optimal level of capability of security solutions for satisfying the optimal amount of investment; (3) The proposed economic model shows that the optimal level of investment in security solutions is an increasing function of vulnerability. However, the optimal level of investment was not proportional to the capability of the integrated security solution; (4) Under various(controllable and uncontrollable) parameters of security solutions, we find the optimal level of the security investment that maximizes the expected net benefits from the investment in the different characteristics of security solutions, i.e., the RSSs and the PSSs. Thus,

given values of various parameters of security solutions, we show that the proposed economic model can be used to help the organization to determine the optimal amount of investment in security solutions.

The rest of the paper is organized as follows. After showing the related works in section 2, we overview the information-theoretic model that quantifies the capability of the integrated security solution in section 3. Using the information-theoretic model, we show the proposed economic model that considers how the capability of the integrated security solution affects the optimal amount of investment in section 4. In section 5, by using the proposed economic model, we describe how to find the optimal amount of IT security investment, which maximizes the expected net benefit, under the influence of various security parameters. Finally, we conclude the paper in section 6.

## 2. RELATED WORK

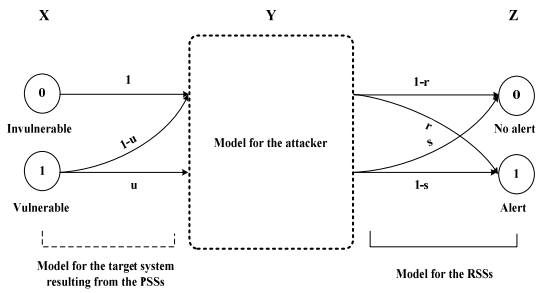
After Moitra et al. found that the increase of the security investment results in the rapid increase of the survivability of organizations from security breaches [16], studies on the investment management on security solutions becomes important. Such studies can be categorized into a qualitative approach and a quantitative approach.

As a qualitative approach, Secure Business Quarterly(SBQ) presents that many of security solutions can complement each other and thus, a comprehensive methodology is required to analyze security investments [17]. Also, Hasan C. et al. presented the importance of four elements of economics of security management, including estimation of breach costs, the strategic nature of security, configuration of security controls, and the complementary and substitute nature of security controls [18]. By investigating the security function from an economic perspective, Hasan C. et al. drew the attention to the economic aspects of IT security management. These qualitative approaches provide a useful starting point for managing the deployment of security solutions. However, since these approaches simply consider the benefits of security investment as an overhead cost and do not quantify the benefits of security investment, they have a limitation in deciding which security solution to deploy or how much to invest.

Many quantitative models from the traditional risk or decision analysis approaches are proposed to overcome the limitation of qualitative approaches. To decide the amount of investment to security solutions, the models identify the potential risks, possible losses and their likelihoods, which are used to compute the expected loss. As a useful method, Longstaff et al. [6] propose Hierarchical Holographic Mode l(HHM), which assesses security risks of IT infrastructure. Gordon and Loeb [7] developed an economic model to determine the optimal level of investment in information security to protect a given set of information. It was found that to maximize the expected benefit from investment, for a given potential loss, it may be better that an organization spends its efforts on information sets with midrange vulnerabilities. However, the traditional risk or decision analysis approaches [6]-[12] have an important limitation that any of those approaches does not determine how the different parameters of security solutions affect the overall security level of the organization and its investment.

As a representative approach to overcome the above limitation, Cavusoglu et al. offered a comprehensive analytical model to evaluate IT security investment decisions using game theory [11]. When designing an analytical metric, Cavusoglu et al. use Bayes Rule that determines the probability of intrusion in the presence(signal) and absence of alerts(no signal) and thus, is used to evaluate the interaction among multiple security solutions. As a result, the model can be used as a guideline to organizations for the optimal configuration of multiple security solutions of the same kind. However, since different decision variables have different improvement results, the model cannot provide any insights for the capability of the integrated security solution whose performance are measured from the combination of decision variables of the different kind. That is, since the PSSs can be evaluated by using the decision variables for reducing the likelihood of successful attack while the RSSs can be evaluated by using the decision variables for detecting and auditing an attack during or after its occurrence, we need the unified model that takes into account all of the decision variables when determining the optimal configuration of multiple security solutions of the different kind.

Note that a cost-benefit analysis is useful for budgeting information security expenditures [14, 15]. In the following sections, we show a comprehensive economic model of the integrated security solution based on the unified model for the integrated security solution. The proposed model considers the relationship between the capability of the integrated security solution from an information-theoretic viewpoint and the investment to the security solution. Thus, the proposed model can be used when organizations determine an optimal amount of IT security investment, where the expected net benefits are maximized, in the PSSs and the RSSs.




(Figure 2) Abstract models for the integrated security solution

# 3. OVERVIEW OF INFORMATION-THEORETIC PERFORMANCE ANALYSIS MODEL

In this section, we overview a quantitative model that analyzes the interactivity of the different security solutions from an information-theoretic viewpoint [19]. Based on the relationship between the security effectiveness(SE) of the security countermeasures and the uncertainty, the information-theoretic analysis model shows how the vulnerability and the potential exploits resulting from such vulnerability can affect their efficiency [13]. Here, the term 'SE' quantifies the efficiency of the security countermeasures.

## 3.1 INFORMATION ENTROPY

Parameters used in this paper are as follows:

- $v$: Probability that IT assets are vulnerable, where $0 \leq v \leq 1$
- $u$: Probability that the PSSs fails at eliminating vulnerabilities of IT assets, where $0 \leq u \leq 1$
- $q$: Probability of vulnerability exploits, where $0 \leq q \leq 1$
- $r$: False positive ratio of the RSSs, where $0 \leq r \leq 1$
- $s$: False negative ratio of the RSSs, where $0 \leq s \leq 1$

In information theory [19], the Shannon entropy H(X) is a measure of the uncertainty associated with a random variable X and the conditional entropy H(X; Y) determines the remaining uncertainty of the input random variable X given the output random variable Y . Here, the Shannon entropy is formulated as

$$H(X) = -\sum_{x \in X} p(x) \log p(x), \quad (1)$$

and the conditional entropy H(X; Y) is formulated as

$$H(X \mid Y) = -\sum_{y \in Y} p(y) \sum_{x \in X} p(x \mid y) \log p(x \mid y), \quad (2)$$

Also, the mutual entropy implies the amount of uncertainty reduction of the input random variable X given the output random variable Y . Here, the mutual entropy is formulated as

$$I(X;Y) = H(X) - H(X \mid Y), \quad (3)$$

where $I(X;Y) = I(Y;X) = H(Y) - H(Y \mid X)$ by symmetry.

## 3.2 CAPABILITY OF INTEGRATED SECURITY SOLUTION

From the abstract model in Figure 2, the uncertainty reduction ratio provided by the integrated security solution is given as follows:

$$U_{PR}(v,u,q,r,s) = \frac{I(X;Z)}{H(X)}, \quad (4)$$

where $0 \leq U_{PR}(v,u,q,r,s) \leq 1$ and the value of p(x) depends on v. We note that the capability of the integrated security solution indicates the capability to correctly identify

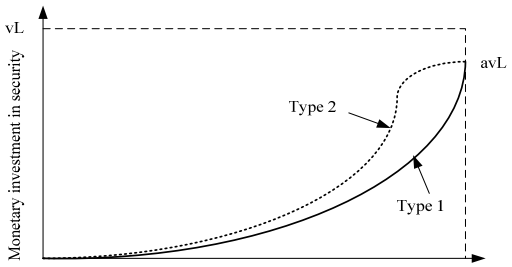
vulnerabilities as vulnerable or invulnerable, and classify the potential exploits from such vulnerabilities as exploit or non-exploit. Based on the information theory, the capability to correctly identify vulnerabilities as vulnerable or invulnerable can be expressed into the uncertainty reduction ratio provided by the PSSs:

$$U_{P|R}(v,u) = I(X;Z) / H(X), \quad (5)$$

This is because the uncertainty reduction ratio provided by the PSSs given the RSSs does not depend on the capability of the RSSs. The capability to classify the potential exploits from such vulnerabilities as exploit or non-exploit can be expressed into the uncertainty reduction ratio provided by the RSSs given the PSSs:

$$U_{R|P}(v,u,q,r,s) = \alpha \cdot \frac{I(Z;Y)}{H(Y)}, \quad (6)$$

where $0 \le I(Z;Y) = I(Y;Z) \le H(Y)$ and $0 \le U_{RP}(v,u,q,r,s) \le 1$. Here, the value of $p(y)$ depends on v, u and q, the value of $p(z \mid y)$ depends on r and s. Also, we denote $\alpha$ $(0 \le \alpha \le 1)$ as the ratio of the capability of the RSSs over the capability of the PSSs since the PSSs actually reduce the likelihood of successful attack while the RSSs detect and audit an attack during or after its occurrence. We note that when we determine the uncertainty reduction ratio resulting from the integrated security solution, the capability of each type of security solutions should be quantified without overlap. Thus, based on the abstract model in Figure 2, we can denote the capability of the integrated security solution as the uncertainty reduction ratio in vulnerabilities.




(Figure 3) An illustration of the relationship between the capability of security solutions and the monetary investment.

# 4. AN ANALYTIC MODEL FOR IT SECURITY INVESTMENT

In this section, we describe the proposed comprehensive economic model that considers how the capability of the integrated security solution affects the optimal amount of investment that should be devoted to securing the IT asset. For this purpose, we consider the relationship between the loss or potential loss associated with the IT asset and the monetary investment in security by comparing the case with security solutions to one without them.

We define the following parameters: L is the loss or potential loss associated with the IT asset and vL is the loss or potential loss associated with the IT asset that is vulnerable with v.

The expected benefits of an investment in the integrated security solution, denoted as EPR, is defined as the reduction in the organization's expected loss attributable to the capability of the integrated security solution given v. Since known vulnerabilities can be eliminated by the PSSs and the potential exploits of the remaining vulnerabilities can be detected and blocked by the RSSs, we assume that the loss or potential loss associated with the IT asset of probability v can be reduced in proportion to $U_{PR}$. Thus, $E_{PR}$ can be expressed as:

$$E_{PR} = vL \times U_{PR}. \quad (7)$$

As $U_{PR}$ is a function of v, u, q, r and s as shown in section 3, the above equation can be expressed as:

$$E_{PR}(U_{PR}(v,u,q,r,s)) = vL \times U_{PR}(v,u,q,r,s). \quad (8)$$

The monetary investment in security to protect the IT asset, denoted as $I_{PR}$, increases as $U_{PR}(v,u,q,r,s)$ increases. More specifically, we note that the monetary investment in security solutions will increase in proportion to the capability of security solutions, but at an increasing rate in the middle of the investment and at a decreasing rate in the beginning of the investment. Thus, we can consider $I_{PR}$ as a function of $U_{PR}(v,u,q,r,s)$, i.e., $I_{PR}(U_{PR}(v,u,q,r,s))$.

The nature of the system vulnerability and the capability of security solutions lead us to consider the following assumptions concerning $I_{PR}(U_{PR}(v,u,q,r,s))$:

1) $I_{PR}(0)=0$. It is clear that without the integrated security solution, the investment will remain zero.
2) $I_{PR}(1)=avL$, where 'a' is a measure of the ratio between the loss or potential loss associated with the IT asset and the monetary cost of the integrated security solution. Here, $0 \le a \le 1$ because for an IT asset with v, the rational decision maker in the organization will not invest a monetary amount in security that exceeds the loss or potential loss associated with the IT asset of v.
3) For all $U_{PR}(v,u,q,r,s)$, $I_{PR}(U_{PR}(v,u,q,r,s))' \ge 0$ and $I_{PR}(U_{PR}(v,u,q,r,s))'' \ge 0$, where $I_{PR}(U_{PR}(v,u,q,r,s))'$ and $I_{PR}(U_{PR}(v,u,q,r,s))''$ denote the first-and second-order derivatives with respect to $U_{PR}(v,u,q,r,s)$, respectively. We assume that compared to the lower $U_{PR}(v,u,q,r,s)$, the cost of the integrated security solution dramatically increases as $U_{PR}(v,u,q,r,s)$ increases. This assumption views the investment in security as an incremental investment beyond the cost of security solutions, specifically their capability.

Based on the above assumptions, we consider an investment function to calculate a closed form solution for the optimal $U_{PR}(v,u,q,r,s)$ and investigate the relationship between SE of the integrated security solution and the security investment. In Figure 3, we show the possible forms of the monetary security investment, where the maximum cost of security solutions cannot exceed vL, because the organization will not invest an excessive amount of money that is larger than the loss or potential loss associated with the IT asset without security solutions. On the contrary to the Type 1 function, the Type 2 function saturates at some sufficiently larger capability of security solutions.

The expected net benefits of an investment in the integrated security solution, denoted as $EN_{PR}(U_{PR}(v,u,q,r,s))$, are the expected values of the investment. That is, $EN_{PR}(U_{PR}(v,u,q,r,s))$ is given as the difference between the expected benefits resulting from the investment in the integrated security solution and the monetary investment itself:

$$EN_{PR}(U_{PR}(v,u,q,r,s)) = E_{PR}(U_{PR}(v,u,q,r,s)) - I_{PR}(U_{PR}(v,u,q,r,s)). \quad (9)$$

From assumption 3), $E_{PR}(U_{PR}(v,u,q,r,s))'' = 0$, $EN_{PR}(U_{PR}(v,u,q,r,s))'' \le 0$, and thus, $E_{PR}(U_{PR}(v,u,q,r,s))$ is a concave function. Hence, an interior maximization is characterized by the first order condition with respect to $U_{PR}(v,u,q,r,s)$. That is,

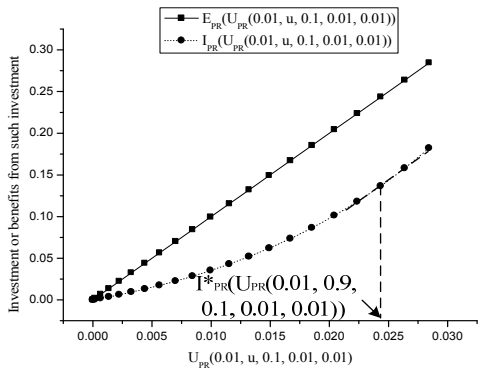
$$\frac{I_{PR}(U_{PR}(v,u,q,r,s))'}{vL} = 1, \quad (10)$$

where the left hand side is the marginal cost of investment (i.e., the cost of increasing $I_{PR}(U_{PR}(v,u,q,r,s))$ by one unit) and the right hand side is the marginal benefit resulting from the security investment in the integrated security solution. Here, we note that $I_{PR}(U_{PR}(v,u,q,r,s))$ measures the monetary investment in security proportional to the capability of the integrated security solution. Thus, based on this assumption, the price of unit of $I_{PR}(U_{PR}(v,u,q,r,s))$ is equal to one, and the marginal cost of investment is also equal to one. Eq. (10) means that one should invest in the integrated security solution only up to the point where the marginal benefit is equal to the marginal cost.

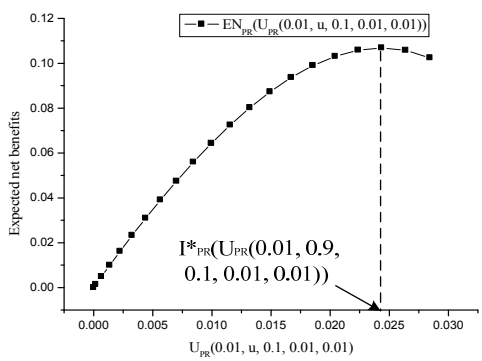
On the basis of the above economic model, we will describe how to determine the optimal level of investment in the integrated security solution in the following section.

## 5. HOW TO DETERMINE IT SECURITY INVESTMENT

From the first-order condition given in Eq. (10), we see that the capability of the integrated security solution influences on the optimal level of investment by affecting the partial derivative of the investment function with respect to $U_{PR}(v,u,q,r,s)$. Also, we observe that the optimal




(a)




(b)

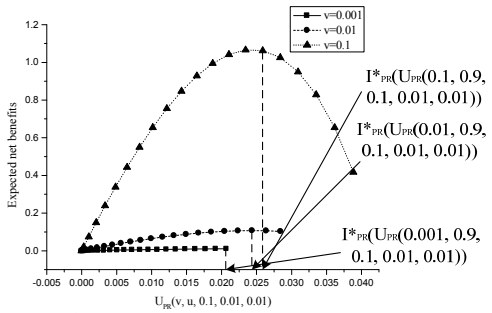
(Figure 4) Influence of u on the benefits and cost of investment in the integrated security solution: (a) Investment or benefits from such investment (b) Expected net benefits.

investment occurs when the difference between the benefits and costs is maximized, which corresponds to the cases when the tangent to $I_{PR}(U_{PR}(v,u,q,r,s))$ has a slope of vL as shown in Eq. (10). Hence, by observing how the expected net benefits resulting from the investment in the integrated security solution vary according to the change in the capability of the integrated security solution, i.e., $U_{PR}(v,u,q,r,s)$, we can find the optimal investment in the integrated security solution and then, the optimal level of the capability of the integrated security solution.

We consider the following cost function for the integrated security solution, which is a Type 1 function, as shown in Figure 3:

$$I_{PR}(U_{PR}(v,u,q,r,s)) = avL \times U_{PR}(v,u,q,r,s) \times e^{b \times U_{PR}(v,u,q,r,s)-1}, \quad (11)$$

where 'b' is a measure of the increase in cost as the $U_{PR}(v,u,q,r,s)$ increases. For the Type 2 function in Figure 3, we can conduct the same analysis, because this type of function is also a convex function.

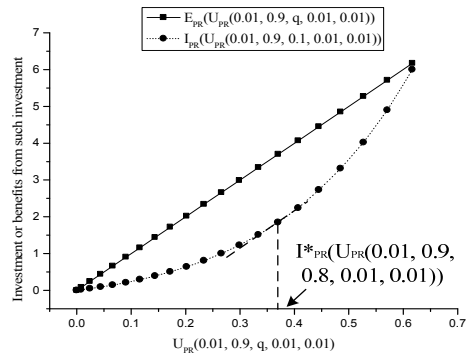



(Figure 5) Influence of v on the optimal IT security investment in the integrated security solution.

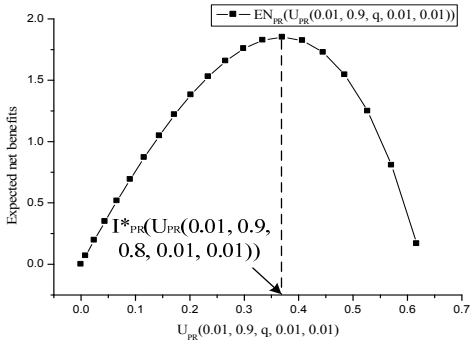
## 5.1 DEFENDER'S VIEW: HOW THE SECURITY SOLUTION(u) AFFECTS THE OPTIMAL IT SECURITY INVESTMENT

The optimal level of investment in the integrated security solution for all $U_{PR}(0.01,u,0.1,0.01,0.01)$ is shown in Figure 4, where a=0.7, b =32 and L=1000. From Eq. (11), the amount of investment starts out at zero and approaches avL as the capability of the integrated security solution increases. Here, the investment dramatically increases at some higher capability of the integrated security solution, where the total amount of investment are constrained at the possible loss vL resulting from v in the absence of any investment in security. Also from Eq. (8), the expected benefits resulting from the investment in the integrated security solution start out at zero when the capability of the integrated security solution is zero and approaches vL as the capability of the integrated security solution increases. Thus, the expected benefits resulting from the investment in the integrated security solution is always higher than the investment in the integrated security solution and thus, the optimal level of investment in the integrated security solution ($I^*_{PR}(U_{PR}(0.01,0.9,0.1,0.01,0.01))$) is found at the point where the

tangent to $I_{PR}(U_{PR}(0.01,u,0.1,0.01,0.01)$ has a slope of vL. Also, as the difference between the benefits and costs is maximized at this point, the optimal capability of security solutions ($U_{PR}(0.01,0.9,0.1,0.01,0.01)$) is found at the same point.




(a)




(b)

(Figure 6) Influence of q on the benefits and cost of investment in the integrated security solution: (a) Investment or benefits from such investment (b) Expected net benefits.

## 5.2 SYSTEM'S VIEW: HOW VULNERABILITY(v) AFFECTS THE OPTIMAL IT SECURITY INVESTMENT

For the integrated security solution, we investigate the influence of vulnerability on the optimal level of investment, i.e., $I^*_{IR}(U_{IR}(v,u,0.1,0.01,0.01))$ by varying the values of v=0.001, 0.01, 0.1 and u from 0 to 1.0 at the increments of 0.05. In Figure 5, it is shown that as v increases, the optimal level of investment in the integrated security solution rapidly increases. This implies that given the high values of vulnerabilities, the organization will benefit from the higher investment. However, it is also shown that the expected net benefit will not increase even though the amount of security investment increases. Since organizations will have a limitation in the security investment subject to budget constraint, this result gives a guideline for the organization to decide the security investment to maximize the expected net benefit.

## 5.3 ATTACKER'S VIEW: HOW VULNERABILITY EXPLOIT(q) AFFECTS THE OPTIMAL IT SECURITY INVESTMENT

In Figure 6, the optimal level of investment in the integrated security solution for all $U_{PR}(0.01,0.9,q,0.01,0.01)$ is shown, where $q \in \{0.1,1.0\}$ in a stepwise manner with step size 0.05, a =0.7, b =2.7 and L =1000. From Figure 6, we assume that the value of u is 0.9, where the optimal capability of the integrated security solution is found in Fig. 4. In Figure 6(a), it is shown that the amount of investment approaches avL as the capability of the integrated security solution increases. Thus, the expected benefits resulting from the investment in the integrated security solution is always higher than the investment in the integrated security solution and thus, the optimal level of investment in the integrated security solution ($I^*_{PR}(U_{PR}(0.01,0.9,0.7,0.01,0.01))$) is found at the point where the tangent to $I_{PR}(U_{PR}(0.01,0.9,q,0.01,0.01))$ has a slope of vL as shown in Figure 6(b). At this point, the optimal capability of the integrated security solution ($U_{PR}(0.01,0.9,0.7,0.01,0.01)$) is found.

# 6. CONCLUSION

To show how the different parameters of the integrated security solution influence on the investment of the organization, we proposed an economic model. By using the proposed economic model, we showed how the capability of the integrated security solution influenced on the optimal amount of investment. Also, we showed how to determine the optimal

condition to maximize the expected net benefits from IT security investment of organizations with respect to the capability of the integrated security solution. Ultimately, we believe that this work will be able to help decision- makers to resolve the poor usage of security budget of organizations based on relationship among input and output parameters of the integrated security solution upon experimenting. After the real relationship between the amount of investment in the integrated security solution and its capability is observed, we would show how the proposed economic model would match the investment and the security.

## Reference


[1] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson, "2006 CSI/FBI Computer Crime and Security Survey," http://americas.utimaco.com/encryption/fbi_csi_2006_p2.html, 2006.

[2] "McAfee threats report", http://www.mcafee.com/us/resources/reports/ rpquarterlythreat-q2-2012.pdf, 2012.

[3] Scott Berinato, "Finally, a real return on security spending," *CIO Magazine*, 2002.

[4] Bodin, L., L. A. Gordon and M. P. Loeb, "Evaluating Information Security Investments Using the Analytical Hierarchy Process," *Communications of the ACM*, 2005.

[5] Campbell, K., L. A. Gordon, M. P. Loeb and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," Journal of Computer Security, vol. 11, no. 3, pp. 431-448, 2003.

[6] Thomas A. Longstaff, Clyde Chittister, Rich Pethia Yacov and Y. Haimes, "Are we forgetting the risk of information technology," *IEEE Computer(The flagship magazine of the IEEE Computer Society)*, vol. 33, no. 12, pp. 43-51, 2000.

[7] Lawrence A. Gordon and Martin P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security (TIScapabilityC)*, vol. 5, no. 4, pp. 438-457, 2002.

[8] Kevin J. Soo Hoo, "How much is enough? A risk management approach to computer security," pages: 100, *Center for International Security And Cooperation (CISAC)*, 2000.

[9] J. E. Gaffney and J. W. Ulvila, "Evaluation of intrusion detectors: A decision theory approach," In Proceedings of the 2001 IEEE Symposium on Security and Privacy, pp. 50-61, 2001.

[10] B. R. Rowe and Michael P. Gallaher, "Private Sector Cyber Security Investment: An Empirical Analysis," *The Fifth Workshop on the Economics of Information Security(WEIS 2006)*, pp. 1-23, 2006.

[11] H. Cavusoglu, B. Mishara, and S. Raghunathan, "A model for evaluating IT security investment," *Communications of the ACM*, vol. 47, no. 7, pp. 87-92, 2004.

[12] Gordon, L. and Loeb, M, "Managing Cybersecurity Resources: A Cost-Benefit Analysis," pages: 211, *McGraw-Hill*, New York, 2006.

[13] Y.-H. Choi, H.-Y. Jeong, S.-W. Seo, "Information-Theoretic Analysis for the Efficiency of the Integrated Security Solutions," *ITC-CSCC 2009*, pp. 1478-1479, 2009.

[14] Gordon, L., Loeb, M. and Lucyshyn, W, "Sharing information on computer systems: An economic analysis," *Journal of Accounting and Public Policy*, vol. 22, no. 6, pp. 461-485, 2003.

[15] Gordon, L. and Loeb, M, "Budgeting process for information security expenditures: Empirical evidence," *Communications of the ACM*, vol. 49, no. 1, pp. 121-125, 2006.

[16] Moitra, S. and Konda, S, "The survivability of network systems: An empirical analysis," *Carnegie Mellon Software Engineering Institute, Technical Report*, CMU/SEI-2000-TR-021, 2000.

[17] Secure Business Quarterly, "Issue on Return on Security Investment (Q4, 2001)," 2001.

[18] Hasan C., Huseyin C. and Srinivasan R, "Economics Of IT Security Management: Four Improvements To Current Security Practices," *Communications of the Association for Information Systems*, vol. 14, pp. 65-75, 2004.

[19] T. Cover, and J. Thomas, "Elements of Information Theory 2/E," pages: 776, *John Wiley & Sons Inc*, 2006.

## ◐ 저 자 소 개 ◑

**최 윤 호 (Yoon-Ho Choi)**

2004년 서울대학교 전기컴퓨터공학부 석사
2008년 서울대학교 전기컴퓨터공학부 박사
2010년 펜실베니아 주립대학교 박사후 연구원
2012년 삼성전자 네트워크 사업부 책임연구원
2012년 - 현재 경기대학교 융합보안학과 조교수
관심분야: 지능형 자동차 IT 보안, 빅데이터, 컴퓨터 및 네트워크 보안 성능 최적화, 보안투자모델링, etc.