Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model

Kanta Matsuura

Institute of Industrial Science, The University of Tokyo
Komaba 4-6-1, Meguro-ku, Tokyo 153-8505, Japan
kanta@iis.u-tokyo.jp

Abstract. Information-security engineers provide some countermeasures so that attacks will fail. This is vulnerability reduction. In addition, they provide other countermeasures so that attacks will not occur. This is threat reduction. Users wish to know how significant these reductions are. One possible approach to the problem of understanding the significance is to ask how the optimal investment strategy for information security is influenced by the reductions. This paper takes that approach by introducing a *productivity space* of information security. In the same manner as in the Gordon-Loeb model where nothing but the vulnerability reduction is considered, I suppose a productivity of information security characterizes an economic effect of information-security investment. In particular, I consider a productivity regarding threat reduction as well as a productivity regarding vulnerability reduction, and investigate a two-dimensional space formed by the two productivities. The main focus in the investigation is on the behavior of the optimal investment in information security in the two-dimensional productivity space. In terms of the behavior, the productivity space is divided into three areas: the no-investment area where both the productivities are low, the mid-vulnerability intensive area where the vulnerability-reduction productivity is high but the threat-reduction productivity is low, and the high-vulnerability intensive area where the threat-reduction productivity is high. The other implications of the model include the importance of public-policy issues regarding investment incentives in the situation where the threat-reduction productivity is low; even outside the no-investment area, when the threat-reduction productivity is below a certain threshold, an increase of productivity could raise the amount of the optimal investment.

1 Introduction

Although security technologies have made great progress in past decades, there are arguments that the security level has scarcely been improved [1]. If there is an algorithm to solve this problem, what we need will be progress in administration[1]. As long as it is hard to find such an algorithm, we need progress in management and evaluation on information security. When one seeks for insights in depth in this direction, economics is helpful [2].

Management and evaluation on information security is a bridge between security engineering and society. On the engineering's side, engineers provide some technologies so that attacks will fail. This is vulnerability reduction. In addition, they provide other technologies so that attacks will not occur. This is threat reduction. We can see the same two reductions also when we consider countermeasures that are not purely technological. On the society's side, users wish to know how significant these reductions are. This paper constructs a simple analytical bridge between the two sides by introducing a *productivity space* of information security.

The first thing to do is to review how the vulnerability reduction and the threat reduction have been studied in the economics of information security so far. Sect. 2 provides that review. We then go on to Sect. 3 where a productivity space of information security is introduced in the context of extending an existing optimal investment model for information security[2]. After implications and limitations of the extended model are mentioned in Sect. 4, concluding remarks are given in Sect. 5.

[1] According to Needham, "Management is that for which there is no algorithm. Where there is an algorithm, it's administration." [2]

[2] The basic concept of the productivity space and relevant theorems will be summarized in the author's short contribution to an honorary volume for a retiring professor, but detailed implications will not be given there. According to the volume editors, the honorary volume welcomes such summaries of the contributors' past or on-going works.

2 The Two Reductions

2.1 Vulnerability Reduction

To inspire managers to information-security risk management, some studies documented the status of information security and potential losses due to security breaches [3], [4], and others showed the return on security investment to convince managers of the benefits of security efforts [5]–[7]. More importantly, managers should know how to appropriately invest in countermeasures to defend against security incidents effectively and efficiently. Some researches use figures and rankings to identify the actual threats and currently available countermeasures [1], [3]. Others provide security management methods and generally prove the efficiency of their methods by conducting a case study in a company or other organizations [8]–[11]. In these qualitative models and heuristic approaches, it is difficult to find a vulnerability-reduction model that is rich in implications.

On the other hand, quantitative models and analytical approaches are relatively fewer, but the most seminal model proposed by Gordon and Loeb [12] has some empirical supports [13], [14]. The essence of the Gordon-Loeb model (GL model, hereafter) is in its formalization regarding the effect of vulnerability reduction. This formalization is extensively helpful in discussing information-sharing and the free-rider problem of information security [15].

Let us consider a one-period economic model of a firm contemplating the additional security efforts to protect a given information set. The information set is characterized by the following three parameters:

λ : the monetary loss conditioned on a breach occurring. It is assumed that λ is a fixed amount as estimated by the firm (for simplicity) and that λ is finite and less than some very large number (so that we can assume risk-neutrality[3]).

t : the threat probability, defined as the probability of a threat occurring. For notational simplicity, they define the potential loss L as $L = t\lambda$. Since t is a probability, $0 \leq t \leq 1$.

v : the vulnerability, defined as the conditional probability that a threat once realized would be successful. Since v is a probability, $0 \leq v \leq 1$.

Let $z > 0$ denote the monetary investment in information security to protect the given information set, measured in the same units (e.g., yen) used to measure the potential loss L. In the GL model, they let $S(z, v)$ denote the probability that the information set will be breached, conditional on the realization of a threat and given that the firm has made an investment of z. $S(z, v)$ is called the security breach probability function (SBP function for short, hereafter). Some classes of functions have been discussed as candidates for the SBP function, and the class of the highest interest among researchers so far is:

$$S(z, v) = v^{\alpha z + 1} \tag{1}$$

where the parameter $\alpha > 0$ is a measure of the productivity of information security regarding vulnerability reduction. The aforementioned interest comes from the fact that this class of SBP function, called the class-II SBP function, has empirical supports [13], [14] and from its implication of an intuitively easy-to-accept strategy: managers allocating an information security budget should normally focus on information which falls into the midrange of vulnerability.

This strategy was derived by solving the maximization problem of ENBIS (Expected Net Benefits from an investment in Information Security):

$$ENBIS(z) = \{v - S(z, v)\} L - z \ \rightarrow \ \max. \tag{2}$$

In summary, the GL model tells that the economic benefit from the information-security investment originates from the reduction of the vulnerability from v to $S(z, v)$.

[3] If someone is *risk-neutral*, it means that they are indifferent to investments that have the same expected value, even though the investments may have varying amounts of risk. By contrast, if someone is *risk-averse*, it means that they would require a higher expected value for an investment with a higher risk.

2.2 Threat Reduction

There are some security technologies that do not reduce vulnerabilities and yet are expected to have other practical effects. A good example is deterrents to Denial-of-Service (DoS) attacks against handshake protocols. One well-known deterrent is a Proof-of-Work (POW) mechanism in which protocol initiators must demonstrate that they have expended processing cost in solving a cryptographic puzzle [16]–[18]. This cost for one execution of the protocol must avoid being prohibitively high because not only DoS attackers but also legitimate users must expend it.

A more traditional POW mechanism is a tool to combat against junk e-mails [19]. In the context of this POW, there have been some economic debates. The point is whether a system with the POW is accepted by users (non-spammers) or not. The answer is not trivial because the extra cost by the POW depends on the statistics of actual traffic and so on.

In 2004, Laurie and Clayton [20] showed that it is not possible to discourage spammers by means of a POW system with keeping an acceptable impact on legitimate users. Their study is based on an economic estimation of the cost of each POW processing, and on a real-world data from a large ISP. Two years later, Liu and Camp [21] showed that POW can work when combined with proper reputation systems. In this series of debate, their interests have been not in the formalization of the effect of the threat reduction but in the numerical estimation of the users' incentive reduction accompanied and how to interpret the estimation results.

3 Productivity Space of Information Security

3.1 Threat-Reduction Productivity

As included in the concluding comments of [12], extension of the GL model is recommendable to study dynamic issues. So let us consider an extension toward the formalization of the effect of the threat reduction.

In particular, let us assume that the information-security investment z can reduce the threat probability and that the reduction depends only on the investment z and the current level of threat probability t. So let $T(z,t)$ denote the probability that a threat occurring, given that the firm has made an investment of z. Let us call $T(z,t)$ the security threat probability function (STP function for short, hereafter). In this extended model, our investment strategy should be discussed by solving the following ENBIS maximization problem:

$$ENBIS(z) = vt\lambda - S(z,v)T(z,t)\lambda - z \ \rightarrow \ \max. \tag{3}$$

By analogy with the empirically-supported class of SBP function, the remainder of this article considers

$$T(z,t) = t^{\beta z+1} \tag{4}$$

where the parameter $\beta \geq 0$ is a measure of the productivity of information security regarding threat reduction. We call α the vulnerability-reduction productivity and β the threat-reduction productivity. The case of $\beta = 0$ corresponds to the original GL model.

The features of the above class of STP function include the followings:

1. $T(z,0) = 0$ for all z. That is, if the information set is completely free from a threat, then it will remain perfectly safe for any amount of information-security investment, including a zero investment.
2. For all t, $T(0,t) = t$. That is, if there is no investment in information security, the threat probability is that inherent to the given information set's environment.
3. For all $t \in (0,1)$, and for all z, we have $T_z(z,t) < 0$ and $T_{zz}(z,t) > 0$, where T_z denotes the partial derivative of T with respect to z and T_{zz} denotes the partial derivative of T_z with respect to z. That is, as the information-security investment increases, the environment gets safer due to the discouragement to attackers, but at a decreasing rate.
4. For all $t \in [0,1)$, $T(z,t) \rightarrow 0$ $(z \rightarrow \infty)$. That is, by investing sufficiently in information security, the threat probability can be made to be arbitrarily close to zero unless the threat is inevitable (*i.e.* $t = 1$).

3.2 Optimal Investment

Let z^* denote the optimal investment as the solution to (3). When we use (1) and (4) in (3), the optimum is characterized by the first-order condition:

$$-\alpha(\ln v)v^{\alpha z+1}t^{\beta z+1}\lambda - \beta(\ln t)v^{\alpha z+1}t^{\beta z+1}\lambda = 1 \tag{5}$$

where the left hand side of (5) represents the marginal benefits from the investment and the right hand side of (5) represents the marginal costs of the investment. However, we must note that the optimal level of investment z^* equals zero if the marginal benefits at $z = 0$ are less than or equal to the marginal costs of such investment. This condition can be rewritten as:

$$F(v) \equiv v\ln v + \frac{\beta\ln t}{\alpha}\cdot v + \frac{1}{\alpha L} \geq 0. \tag{6}$$

When $F(v) < 0$, from (5), we have

$$z^* = \frac{\ln\left\{-1/\left(vt\lambda\ln(v^\alpha t^\beta)\right)\right\}}{\ln(v^\alpha t^\beta)} = \frac{\ln\frac{1}{-vL\{\alpha(\ln v)+\beta(\ln t)\}}}{\alpha(\ln v)+\beta(\ln t)}. \tag{7}$$

3.3 Productivity Space

Let us investigate how the optimal level of investment z^* behaves for different values of the productivities α and β of information security. To see this, knowing the characteristics of the function $F(v)$ is helpful.

First, since $F(v) \to \frac{1}{\alpha L}$ $(v \to +0)$, we find $z^* \to 0$ when $v \to +0$.

Second, we have its derivative as

$$F'(v) = \frac{\beta\ln t}{\alpha} + \ln v + 1. \tag{8}$$

So by letting $v_0 = e^{-1-(\beta\ln t)/\alpha}$, we have $F'(v) = 0 \Leftrightarrow v = v_0$. Paying attention to the fact $F''(v) = 1/v > 0$ and the equivalence

$$F(v_0) = \frac{1}{\alpha L} - e^{-1-(\beta\ln t)/\alpha} \geq 0 \Leftrightarrow \beta \leq \frac{\alpha(\ln\alpha L - 1)}{\ln t}, \tag{9}$$

we can see the following breakdown is helpful in the investigation[4].

(Case I) When $F(v_0) \geq 0$;

To help the observation in the α-β plane, this condition can be rewritten as $\beta \leq \frac{\alpha(\ln\alpha L-1)}{\ln t}$.

Since $F(v) \geq F(v_0) \geq 0$, (6) holds and hence $z^* = 0$.

(Case II) When $F(v_0) < 0$;

Likewise, this condition can be rewritten as $\beta > \frac{\alpha(\ln\alpha L-1)}{\ln t}$.

From $F(v_0) = \frac{1}{\alpha L} - v_0 < 0$, we have $v_0 > \frac{1}{\alpha L}$.

(Case II-A) When $\frac{1}{\alpha L} \geq 1$ in addition to the condition of Case II;

This additional condition can be rewritten as $\alpha \leq 1/L$.

From $\alpha \leq 1/L$ and $v_0 > \frac{1}{\alpha L}$, we have $v_0 > 1$.

Therefore, the minimum of $F(v)$ is $F(1) = \frac{\beta\ln t}{\alpha} + \frac{1}{\alpha L}$.

(Case II-A-1) When $\beta \leq -1/(L\ln t)$ in addition to the condition of Case II-A;

Since $F(v) \geq F(1) \geq 0$, (6) holds and hence $z^* = 0$.

(Case II-A-2) When $\beta > -1/(L\ln t)$ in addition to the condition of Case II-A;

Since $F(1) < 0$, there exists $V_1 \in (0,1)$ such that

- For the region $0 < v \leq V_1$, (6) holds and hence $z^* = 0$.
- For the region $V_1 < v \leq 1$, (6) does not hold and hence $z^* > 0$ is given by (7).

(Case II-B) When $\alpha > 1/L$ in addition to the condition of Case II;

Paying attention to $v_0 \geq 1 \Leftrightarrow \beta \geq -\alpha/\ln t$, we divide this case into the following subcases.

[4] The mathematical details are not appended at the end of the paper but shown here in line so that readers can follow the case-breakdown smoothly.

(Case II-B-1) When $\beta \geq -\alpha/\ln t$ in addition to the condition of Case II-B;
$v_0 \geq 1$ and therefore the minimum of $F(v)$ is $F(1) = \frac{\beta \ln t}{\alpha} + \frac{1}{\alpha L}$.
Since $\alpha > 1/L$, we have $\beta + \frac{1}{L \ln t} > \beta + \frac{\alpha}{\ln t} \geq 0$, and hence

$$F(1) < -\frac{1}{L \ln t} \cdot \frac{\ln t}{\alpha} + \frac{1}{\alpha L} = 0. \tag{10}$$

Therefore, there exists $V_1 \in (0, 1)$ such that
- For the region $0 < v \leq V_1$, (6) holds and hence $z^* = 0$.
- For the region $V_1 < v \leq 1$, (6) does not hold and hence $z^* > 0$ is given by (7).

(Case II-B-2) When $\beta < -\alpha/\ln t$ in addition to the condition of Case II-B;
Since $v_0 < 1$, the minimum of $F(v)$ is $F(v_0) < 0$. So paying attention to $F(1) = \frac{\beta \ln t}{\alpha} + \frac{1}{\alpha L}$, we find the following.

(Case II-B-2-a) When $F(1) > 0$ in addition to the condition of Case II-B-2;
$\beta < -1/(L \ln t)$ since $F(1) > 0$.
There exist V_1 and V_2 such that $0 < V_1 < V_2 < 1$ and
- For the regions $0 < v \leq V_1$ and $V_2 \leq v \leq 1$, (6) holds and hence $z^* = 0$.
- For the region $V_1 < v < V_2$, (6) does not hold and hence $z^* > 0$ is given by (7).

(Case II-B-2-b) When $F(1) \leq 0$ in addition to the condition of Case II-B-2;
$\beta \geq -1/(L \ln t)$ since $F(1) \leq 0$.
There exists V_1 such that $0 < V_1 < v_0 < 1$ and
- For the region $0 < v \leq V_1$, (6) holds and hence $z^* = 0$.
- For the region $V_1 < v \leq 1$, (6) does not hold and hence $z^* > 0$ is given by (7).

The cases investigated above can be recognized as illustrated in Fig. 1.

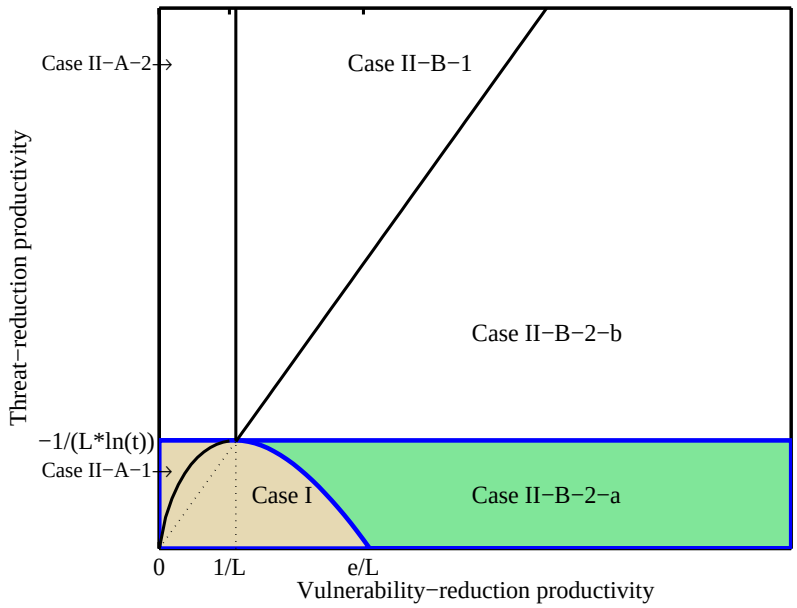

Fig. 1. Productivity space of information security, divided into three areas of different colors: the lower left area composed of Case I and Case II-A-1 is a no-investment area, the lower right area composed of Case II-B-2-a is a mid-vulnerability intensive area, and the upper large area composed of Case II-A-2, Case II-B-1, and Case II-B-2-b is a high-vulnerability intensive area. The situation studied by the class-II SBP function in the original Gordon-Loeb model is included in the mid-vulnerability intensive area, on the horizontal axis.

The lower left area composed of Case I and Case II-A-1 is a no-investment area; the optimal investment z^* equals zero regardless of the vulnerability v. A numerical example in this area is given in Fig. 2. The curve

$$-\alpha v \ln v - \beta v \ln t$$

is shown in Fig. 2 so that one can see whether (6) holds or not at a glance; (6) is equivalent to

$$-\alpha v \ln v - \beta v \ln t \leq \frac{1}{L}. \tag{11}$$

The lower right area composed of Case II-B-2-a is a mid-vulnerability intensive area; the optimal investment z^* equals zero for low ($v \leq V_1$) and high ($v \geq V_2$) vulnerabilities whereas the investment occurs ($z^* > 0$) intensively for the midrange ($V_1 < v < V_2$) vulnerabilities. For these midrange vulnerabilities, the curve exceeds $1/L$ (that is, (6) does not hold), and hence the optimal investment is given by (7). In particular, the α-axis in this region (that is, the case when $\beta = 0$ and $\alpha > e/L$) corresponds to the situation well-discussed by Gordon and Loeb [12]. A numerical example in this area is given in Fig. 3.

The upper large area composed of Case II-A-2, Case II-B-1, and Case II-B-2-b is a high-vulnerability intensive area; the optimal investment z^* equals zero for low ($v \leq V_1$) vulnerabilities whereas the investment occurs ($z^* > 0$) for higher ($v > V_1$) vulnerabilities. A numerical example in this area is given in Fig. 4. The feature shown here is similar to that of the SBP function of class I in [12]; a firm can be better off concentrating its security resources on high-vulnerability information sets. It is remarkable that this happens in spite of the same values of the potential loss L and the vulnerability-reduction productivity α as in [12]. The very high information-security productivity β regarding threat reduction causes this intensity shift from midrange vulnerabilities to high vulnerabilities.

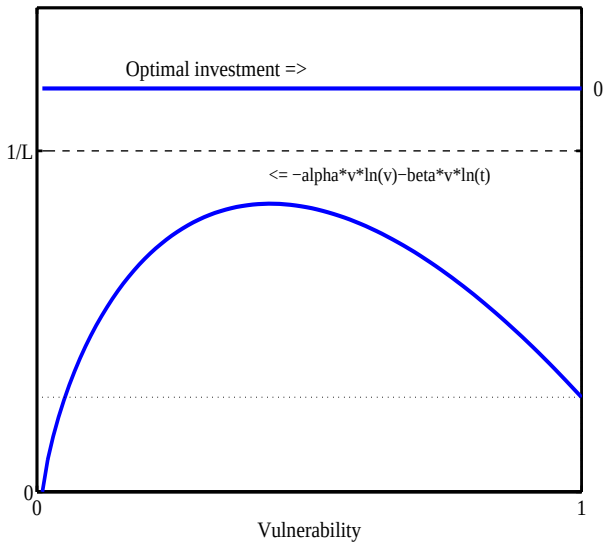

Fig. 2. A numerical example of the no-investment area ($\alpha = 0.000005$, $\beta = 0.000001$, $t = 0.5$, $\lambda = 800000$). The curve $-\alpha v \ln v - \beta v \ln t$ (its values are labeled on the left vertical axis) as well as the optimal investment (labeled on the right vertical axis) is shown so that one can see whether (6) holds or not at a glance. In this numerical example, the curve never exceeds $1/L$ regardless of the value of the vulnerability. This means (6) holds for any $v \in (0, 1]$, and hence the optimal investment is given by $z^* = 0$. Intuitively, both the productivities are too low and there is no incentive for information security. It should be noted that this happens for the same potential loss L as in the page 449 of [12] and the vulnerability-reduction productivity α about as half as there.

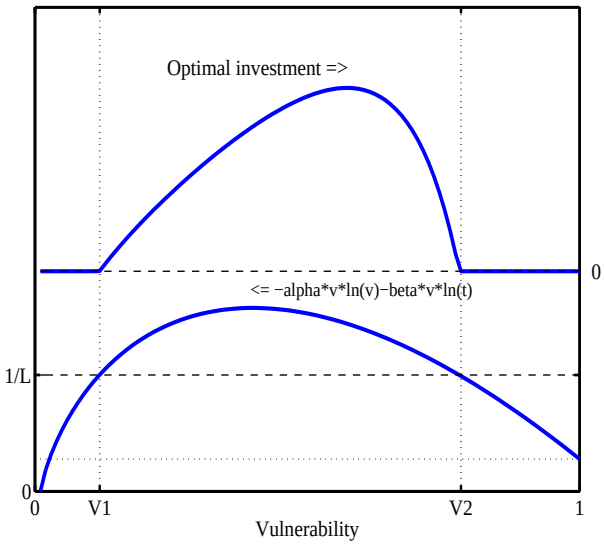

Fig. 3. A numerical example of the mid-vulnerability intensive area ($\alpha = 0.00001$, $\beta = 0.000001$, $t = 0.5$, $\lambda = 800000$). In the same way as in [12], this shows an intuitively easy-to-accept strategy: managers allocating an information security budget should normally focus on information which falls into the midrange of vulnerability.

Our next interest is in the effects of productivity improvement on the optimal investment z^* when $z^* > 0$. To investigate this, by elementary calculus, we have

$$\frac{\partial z^*}{\partial \alpha} \geq 0 \Leftrightarrow \frac{\partial z^*}{\partial \beta} \geq 0 \Leftrightarrow -v \ln v \leq \frac{\beta \ln t}{\alpha} \cdot v + \frac{e}{\alpha L} \tag{12}$$

from (7). One can observe that replacing L with L/e in (6) yields the inequality of the right hand side of (12). So based on a similar investigation to that from Case I to Case II-B-2-b, we achieve the following theorems.

Theorem 1. *Suppose the information-security productivities satisfy the condition*

$$\left(\frac{e}{L} < \alpha\right) \bigwedge \left(\frac{\alpha(\ln(\alpha L/e) - 1)}{\ln t} < \beta < -e/(L \ln t)\right).$$

Then there exist V_3 and V_4 such that $0 < V_3 < V_4 < 1$ and

- *For the regions $0 < v \leq V_3$ and $V_4 \leq v < 1$, when the optimal investment $z^* > 0$, z^* could increase as the productivities increase (that is, $\frac{\partial z^*}{\partial \alpha} \geq 0$ and $\frac{\partial z^*}{\partial \beta} \geq 0$).*
- *For the region $V_3 < v < V_4$, when the optimal investment $z^* > 0$, z^* decreases as the productivities increase (that is, $\frac{\partial z^*}{\partial \alpha} < 0$ and $\frac{\partial z^*}{\partial \beta} < 0$).*

Theorem 2. *Suppose the information-security productivities satisfy the condition*

$$\left(\left(\alpha \leq \frac{e^2}{L}\right) \bigwedge \left(\beta \leq \frac{\alpha(\ln(\alpha L/e) - 1)}{\ln t}\right)\right) \bigvee \left(\left(\alpha \leq \frac{e}{L}\right) \bigwedge \left(\frac{\alpha(\ln(\alpha L/e) - 1)}{\ln t} < \beta < -\frac{e}{L \ln t}\right)\right).$$

Then, for any v, when the optimal investment $z^* > 0$, z^* could increase as the productivities increase (that is, $\frac{\partial z^*}{\partial \alpha} \geq 0$ and $\frac{\partial z^*}{\partial \beta} \geq 0$).

The numerical example used for Fig. 3 satisfies the condition in Theorem 2.

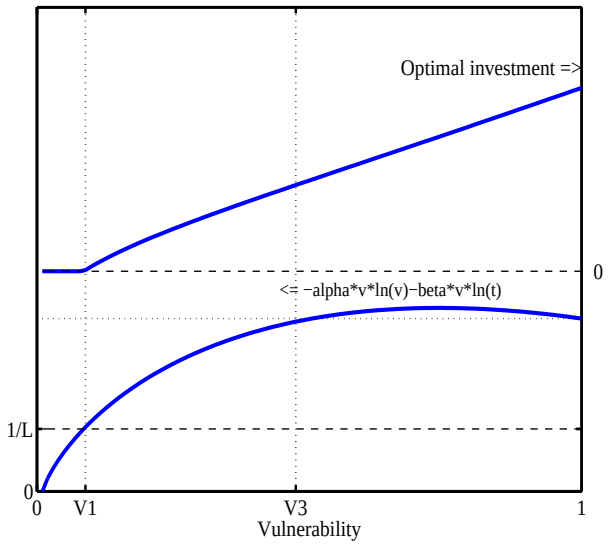

Fig. 4. A numerical example of the high-vulnerability intensive area ($\alpha = 0.00001$, $\beta = 0.00001$, $t = 0.5$, $\lambda = 800000$). The feature shown here is similar to that of the SBP function of class I in [12]. The meaning of the vulnerability value V_3 will appear in Theorem 3.

Theorem 3. *Suppose the threat-reduction productivity satisfies the condition*

$$\beta > -\frac{e}{L \ln t}.$$

Then there exists $V_3 \in (0,1)$ *such that*

- *For the region* $0 < v \leq V_3$*, when the optimal investment* $z^* > 0$*,* z^* *could increase as the productivities increase (that is,* $\frac{\partial z^*}{\partial \alpha} \geq 0$ *and* $\frac{\partial z^*}{\partial \beta} \geq 0$*).*
- *For the region* $V_3 < v < 1$*, when the optimal investment* $z^* > 0$*,* z^* *decreases as the productivities increase (that is,* $\frac{\partial z^*}{\partial \alpha} < 0$ *and* $\frac{\partial z^*}{\partial \beta} < 0$*).*

The numerical example used for Fig. 4 satisfies the condition in Theorem 3, and the parameter V_3 is indicated on the horizontal axis of Fig. 4 for reference.

4 Implications and Limitations

4.1 Different Investment Strategies

We must remember that Gordon and Loeb [12] showed different classes of SBP functions can bring different investment strategies such as mid-vulnerability intensive one and high-vulnerability intensive one. By contrast, the formalization of threat reduction in this paper tells us that not only different classes of functions but also different values of productivities can support different investment strategies.

4.2 Influence of Productivity-Assessment Failures

Let us regard the no-investment strategy as a special case of the mid-vulnerability intensive strategy as well as of the high-vulnerability intensive strategy. Suppose that we are trying to choose one of the two strategies, mid- and high-vulnerability intensive strategies, by assessing the productivities of information security. In the original GL model, we do not have to be afraid of a wrong choice being caused by assessment failure.

However, in our extended model, a failure in assessing the threat-reduction productivity, β, can lead us to a wrong choice. If the actual vulnerability-reduction productivity α is larger than e/L and the actual threat-reduction productivity β is larger than $-1/\{L \ln(t)\}$, then an underestimate of the latter such

that $\beta < -1/\{L\ln(t)\}$ brings a wrong strategy of recommending the focus on midrange vulnerabilities. Likewise, if the actual vulnerability-reduction productivity α is larger than e/L and the actual threat-reduction productivity β is smaller than $-1/\{L\ln(t)\}$, then an overestimate of the latter such that $\beta > -1/\{L\ln(t)\}$ brings a wrong strategy of recommending the focus on high vulnerabilities. To our annoyance, the threshold value $-1/\{L\ln(t)\}$ depends on parameters that are also to be assessed. In light of this, our future work of empirical studies must be carefully designed.

4.3 Upper Limit of the Optimal Investment

An important implication of the original GL model is the relationship between z^*, the optimal level of security investment, and $vt\lambda$, the loss that would be expected in the absence of any security investment when the SBP functions belong to two particular classes including the one used in this paper. In the case of the two classes, called class I and class II, the optimal investment in information security is always less than or equal to 36.79% (i.e. $1/e$) of $vt\lambda$. Our extended model has the same upper limit of the optimal investment; from (7), it is elementary to observe that we can use the same proof technique[5] as the one used for the class II SBP function in the GL model.

4.4 Influence of Technology Innovation

When an innovation of information-security technologies happens, we expect that productivities of information security are increased. When we discuss the influence of the technology innovation on information-security investment, we must be careful about our current location in the productivity space of information security. This is because the location determines the recommended investment strategy (no investment, mid-vulnerability intensive, or high-vulnerability intensive) and which condition in Theorems 1–3 is satisfied.

Let us look at Fig. 5 that revisits the productivity space with auxiliary dashed lines intended for easier reading of Theorems 1–3.

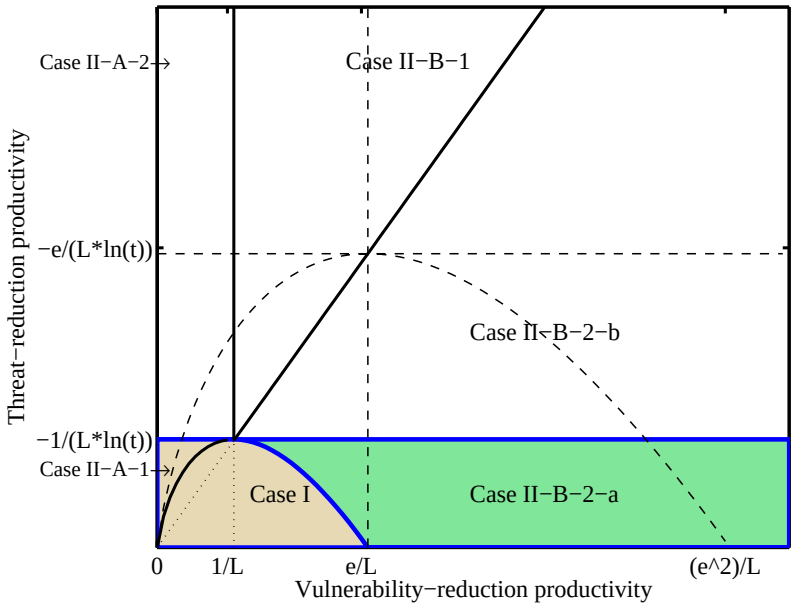

Fig. 5. Productivity space of information security, divided into three areas of different colors: the lower left area composed of Case I and Case II-A-1 is a no-investment area, the lower right area composed of Case II-B-2-a is a mid-vulnerability intensive area, and the upper large area composed of Case II-A-2, Case II-B-1, and Case II-B-2-b is a high-vulnerability intensive area. Auxiliary dashed lines are appended to help easier reading of Theorems 1–3.

[5] Divide (7) by vL and then let $x = -vL\{\alpha(\ln v) + \beta(\ln t)\}$.

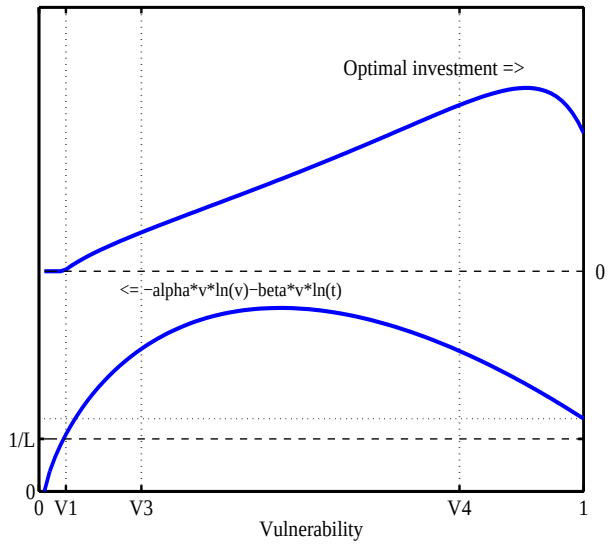

Fig. 6. Another numerical example of the high-vulnerability intensive area ($\alpha = 0.00002$, $\beta = 0.000005$, $t = 0.5$, $\lambda = 800000$). Whereas the former example in Fig. 4 satisfies the condition in Theorem 3, this example satisfies the condition in Theorem 1. For high vulnerabilities such that $v > V_4$, we have $\frac{\partial z^*}{\partial \alpha} \geq 0$ and $\frac{\partial z^*}{\partial \beta} \geq 0$.

When $e/L < \alpha$ and $\max\{\frac{\alpha(\ln(\alpha L/e)-1)}{\ln t}, -1/(L\ln t)\} < \beta < -e/(L\ln t)$, the point (α, β) is in the high-vulnerability intensive area. In addition, this situation satisfies the condition of Theorem 1. Suppose that information-security investment is focused on high vulnerabilities, say, $v > V_4$. Then, from Theorem 1, we have $\frac{\partial z^*}{\partial \alpha} \geq 0$ and $\frac{\partial z^*}{\partial \beta} \geq 0$. Therefore, when an innovation increases information-security productivities, the optimal amount of investment could be increased. A numerical example for this situation is shown in Fig. 6

When $e/L < \alpha$ and $\frac{\alpha(\ln(\alpha L/e)-1)}{\ln t} < \beta < -1/(L\ln t)$, the point (α, β) is in the mid-vulnerability intensive area. In addition, this situation satisfies the condition of Theorem 1. Suppose a strategy of information-security investment focused on midrange vulnerabilities, say, $V_3 < v < V_4$. Then, from Theorem 1, we have $\frac{\partial z^*}{\partial \alpha} < 0$ and $\frac{\partial z^*}{\partial \beta} < 0$. Therefore, when an innovation increases information-security productivities, the optimal amount of investment is decreased.

However, we must be careful whether the strategy above is realistic or not. In fact, if one rather chooses a strategy of focusing sharply around the maximum of the optimal-investment curve, the focus is outside the vulnerability range $V_3 < v < V_4$ (see an example shown in Fig. 7). The reason is the following. From (7), we have

$$\frac{\partial z^*}{\partial v} = \frac{-\left\{\frac{1}{v} - \frac{\alpha/v}{\alpha(\ln v)+\beta(\ln t)}\right\} \cdot \{\alpha(\ln v) + \beta(\ln t)\} + \{\ln(vL) + \ln(-\alpha(\ln v) - \beta(\ln t))\} \cdot \frac{\alpha}{v}}{\{\alpha(\ln v) + \beta(\ln t)\}^2}. \tag{13}$$

For $v \in (0,1)$, due to the fact that $\alpha/v > 0$ and $\{\alpha(\ln v) + \beta(\ln t)\}^2 > 0$, the sign of (13) is given by the sign of

$$G(v) \equiv -\frac{\alpha(\ln v) + \beta(\ln t)}{\alpha} + 1 + \ln(vL) + \ln(-\alpha(\ln v) - \beta(\ln t)) \tag{14}$$

$$= -\frac{\beta \ln t}{\alpha} + 1 + \ln L + \ln(-\alpha(\ln v) - \beta(\ln t)) \tag{15}$$

This function $G(v)$ is monotonically decreasing for $v \in (0,1)$, and $G(v) \to \infty$ when $v \to +0$. Therefore, with the help of (12), we can see that

$$(G(V_5) = 0) \bigwedge \left(-V_5 \ln V_5 > \frac{\beta \ln t}{\alpha} \cdot V_5 + \frac{e}{\alpha L}\right) \tag{16}$$

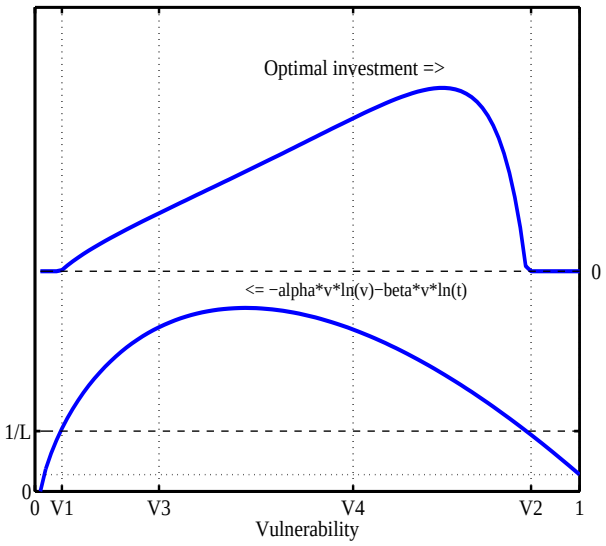

Fig. 7. Another numerical example of the mid-vulnerability intensive area ($\alpha = 0.00002$, $\beta = 0.000001$, $t = 0.5$, $\lambda = 800000$). Whereas the former example in Fig. 3 satisfies the condition in Theorem 2, this example satisfies the condition in Theorem 1. For relatively high vulnerabilities such that $V_4 < v < V_2$, we have $\frac{\partial z^*}{\partial \alpha} \geq 0$ and $\frac{\partial z^*}{\partial \beta} \geq 0$.

is a necessary condition for z^* to take a maximum at $v = V_5$ such that $V_3 < V_5 < V_4$ and the point (α, β) is in the mid-vulnerability intensive area. From $G(V_5) = 0$, we have

$$-\alpha(\ln V_5) - \beta(\ln t) = \frac{t^{\frac{\beta}{\alpha}}}{eL}. \tag{17}$$

Regarding the latter part of the necessary condition (16), since $\alpha/V_5 > 0$, we have

$$-V_5 \ln V_5 > \frac{\beta \ln t}{\alpha} \cdot V_5 + \frac{e}{\alpha L} \Leftrightarrow -\alpha(\ln V_5) - \beta(\ln t) > \frac{e}{LV_5} \tag{18}$$

Using (17) in (18), we have

$$\frac{t^{\frac{\beta}{\alpha}}}{eL} > \frac{e}{LV_5} \tag{19}$$

That is,

$$t^{\frac{\beta}{\alpha}} > \frac{e^2}{V_5} \tag{20}$$

Since $0 \leq t \leq 1$ tells $t^{\frac{\beta}{\alpha}} \leq 1$ and $0 < V_5 < 1$ tells $\frac{e^2}{V_5} > 1$, the inequality (20) is a contradiction.

When $\beta > -e/(L \ln t)$, the point (α, β) is in the high-vulnerability intensive area. In addition, this situation satisfies the condition of Theorem 3. Suppose that information-security investment is focused on high vulnerabilities, say, $v > V_3$. Then, from Theorem 3, we have $\frac{\partial z^*}{\partial \alpha} < 0$ and $\frac{\partial z^*}{\partial \beta} < 0$. Therefore, when an innovation increases information-security productivities, the optimal amount of investment is decreased. In other words, our location in the productivity space is in a cost-saving region where innovation could allow us to reduce information-security investment. This situation was visited by Fig. 4.

In the situations that have not been described above, except the no-investment area, the condition of Theorem 2 is satisfied. So whichever vulnerability range is focused, we have $\frac{\partial z^*}{\partial \alpha} \geq 0$ and $\frac{\partial z^*}{\partial \beta} \geq 0$ from Theorem 2. Therefore, when an innovation increases information-security productivities, the optimal amount of investment could be increased.

Figure 8 is described to summarize the observations above. If information-security countermeasures are poor and both the productivities are low, risk-neutral users would likely find it hard to have good incentives to information-security efforts. Therefore, in order to enhance the efforts, policy issues regarding implementation of some other good incentive mechanisms should be considered in such low-productivity situations. In addition, it should be noted that the white and the light-gray regions stretch out toward

further right in Fig. 8; even when the vulnerability-reduction productivity is high, low productivities regarding threat reduction could cause a similar need of incentive mechanisms.

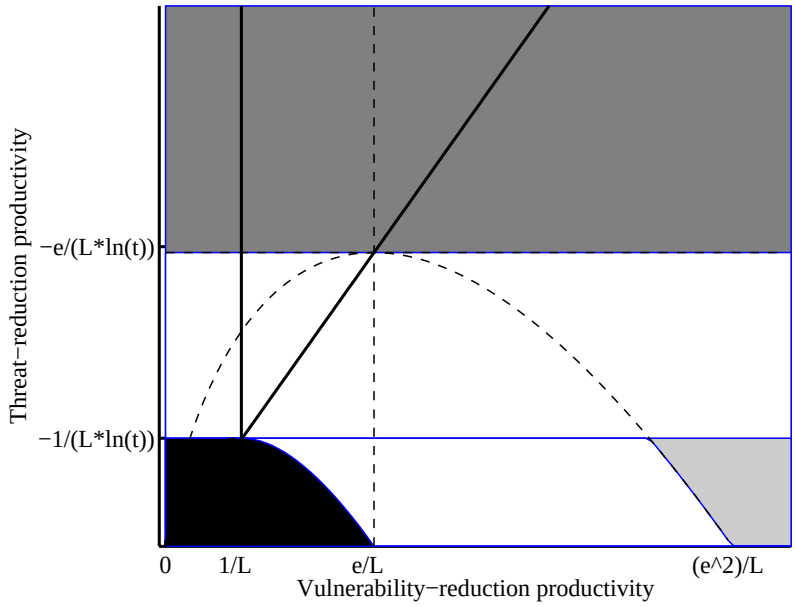

Fig. 8. Productivity space of information security, divided into four regions. The first one is a cost-saving region (painted dark gray in this figure) where the increase of information-security productivities would reduce the amount of the optimal investment determined by the suggested investment strategy of the model. In the second region (painted light gray in this figure), the change of the optimal investment in response to productivity increase would strongly depend on how we interpret the midrange vulnerabilities. In the third region (white in this figure), the increase of information-security productivities would raise the optimal investment, which could do harm to incentives to information-security efforts. The final one (black region) is simply the no-investment region where the optimal investment is zero.

4.5 Tradeoff between Vulnerability Reduction and Threat Reduction

Suppose that a family bought a watchdog. If their house is a *little house on the prairie*, then the resultant threat reduction would be discouragement of burgling into the little house only. On the other hand, if the house is a small one in an densely-populated urban area, then the threat-reduction effect, burglar discouragement, would reach its neighborhood as well; burglars would hesitate to attack not only the house where the watchdog is introduced but also other houses nearby.

In the latter case, there will be a clear tradeoff between vulnerability reduction and threat reduction; if one expects a strong threat reduction on him by other parties' investment, and if he likewise expects a strong threat reduction on other parties by his investment, then he may reduce his incentive for the security investment. Thus, even though the vulnerability reduction is a positive incentive factor, we will face a tradeoff if we consider the threat reduction as well. Of course, an analysis of free-riding problem related to this tradeoff will be an interesting research topic.

However, in this article, the proposed model considers the former case (the "little house on the prairie" model). And hence, the model does not directly address the tradeoff. Although this is a limitation of the model at present, the author expects that a generalization is possible to study the latter model (the "Japanese *rabbit-hutch* house[6]" model), for example in a similar way to the reformulation[15] of the original GL model; in [15], they reformulated the original GL model to study the vulnerability reduction on other parties through information sharing.

[6] Small houses densely located in Japanese large cities are sometimes called "rabbit hutches."

5 Concluding Remarks

In the context of extending the Gordon-Loeb model, this paper introduced the concept of productivity space of information security, and investigated the behavior of the optimal information-security investment there. Security efforts can reduce vulnerabilities. Security efforts can reduce threats. The productivities regarding these two reductions can be enhanced by research, innovation, well-designed public policies, and so on. The optimal investment strategies for different vulnerabilities are characterized by a space formed by these productivities. Although restricted to risk-neutral users and a particular class of functions in the model, it is suggested that implementation of incentive mechanisms other than those resulting from the model would be important at least when our location in the productivity space is closer to lower-left area; as easily acceptable by our intuition, public-policy issues regarding incentive mechanisms would be more important in the situations of less matured information-security productivities. In addition, even when the vulnerability-reduction productivity is high, low productivities regarding threat reduction could cause a similar need of incentive mechanisms. Future studies would include a reformulation of the model to directly address the tradeoff between vulnerability reduction and threat reduction.

Acknowledgement.
The author is grateful to anonymous reviewers for their productive comments. This work is partly supported by Young-Researcher Grant from NEDO (New Energy and Industrial Technology Development Organization) of Japan.

References

1. Whitman, M. E.: Enemy at the gate: threats to information security. Comm. ACM **46** (2003) 91–95
2. Anderson, R. J.: Security engineering: a guide to building dependable distributed systems. John Wiley & Sons (2001)
3. Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Richardson, R.: 2005 CSI/FBI Computer Crime and Security Survey. Computer Security Institute (2005)
4. Kuper, P.: The status of security. IEEE Security & Privacy **3** (2005) 51–53
5. Purser, S. A.: Improving the ROI of the security management process. Computers & Security **23** (2004) 542–546
6. Hoo, K. S., Sudbury, A. W. and Jaquith, A. R.: Tangible ROI through secure software engineering. Security Business Quarterly **1**, Fourth Quarter (2001)
7. Geer, D. E.: Making choices to show ROI. Security Business Quarterly **1**, Fourth Quarter (2001)
8. Kim, S. and Lee, H. J.: Cost-benefit analysis of security investments: methodology and case study. LNCS 3482 (2005) 1239–1248
9. Karabacak, B. and Sogukpinar, L.: ISRAM: information security risk analysis method. Computers & Security **24** (2005) 147–159
10. Dynes, S., Brechbuhl, H. and Johnson, M. E.: Information security in the extended enterprise: some initial results from a field study of an industrial firm. 2005 Workshop on the Economics of Information Security (2005)
11. Lovea, P. E. D., Iranib, Z., Standinga, C., Lina, C. and Burna, J. M.: The enigma of evaluation: benefits, costs and risks of IT in Australian small-medium-sized enterprises. Information & Management **42** (2005) 947–964
12. Gordon, L. A. and Loeb, M. P.: The economics of information security investment. ACM Trans. on Info. & Sys. Sec. **5** (2002) 438–457
13. Tanaka, H., Matsuura, K. and Sudoh, O.: Vulnerability and information security investment: an empirical analysis of e-local government in Japan. Journal of Accounting and Public Policy **24** (2005) 37–59
14. Liu, W., Tanaka, H. and Matsuura, K.: Empirical-analysis methodology for information-security investment and its application to a reliable survey of Japanese firms. IPSJ Journal **48** (2007) 3204-3218
15. Gordon, L. A., Loeb, M. P. and Lucyshyn, W.: Sharing information on computer systems security: An economic analysis. Journal of Accounting & Public Policy **22** (2003) 461–485
16. Matsuura, K. and Imai, H.: Protection of authenticated key-agreement protocol against a Denial-of-Service attack. Proc. of the 1998 International Symposium on Information Theory and Its Applications (1998) 466–470
17. Matsuura, K. and Imai, H.: Modified aggressive modes of Internet Key Exchange resistant against Denial-of-Service attacks. IEICE Trans. Info. Sys. **E83-D** (2000) 972–979
18. Juels, A. and Brainard, J.: Client puzzles: a cryptographic countermeasure against connection depletion attacks. Proc. of the Network and Distributed System Security Symposium (1999) 151–165

19. Dwork, C. and Naor, M.: Pricing via processing or combatting junk mail. LNCS 740 (1992) 139–147
20. Laurie, B. and Clayton, R.: "Proof-of-Work" proves not to work. 2004 Workshop on the Economics of Information Security (2004)
21. Liu, D. and Camp, L. J.: Proof of Work can work. 2006 Workshop on the Economics of Information Security (2006)