Optimal Timing of Information Security Investment: A Real Options Approach

Ken-ichi TATSUMI (corresponding author)
Faculty of Economics, Gakushuin University,
Mejiro 1-5-1, Toshima-ku, Tokyo 171-8588, Japan
E-mail: Kenichi.Tatsumi@gakushuin.ac.jp

Makoto GOTO
Graduate School of Finance, Accounting and Law, Waseda University
1-4-1 Nihombashi, Chuo-ku, Tokyo 103-0027, Japan
E-mail: mako.50@aoni.waseda.jp

July 21, 2009 (earlier version: May 18, 2009)

Keywords: real options, information security investment, threat,
JEL(s): D24, D81, E22, L86, M15.

Abstract: This paper applies real options analytic framework to firms' investment activity in information security technology and then a dynamic analysis of information security investment is explored by extending Gordon-Loeb (2002). The current research provides how firms have to respond to immediate or remote threat numerically. It shows that although positive drift of threat causes both larger and later investment expenditure, negative drift causes immediate investment and lower investment expenditure. The efficiency of vulnerability reduction technology encourages firms to invest earlier and induces cost reduction. To know the form of vulnerability is important because the effect of high vulnerability on timing and amount of the investment expenditure is mixed.

---

*) Advices by anonymous reviewers are gratefully acknowledged. All remaining errors are our own.

Optimal Timing of Information Security Investment: A Real Options Approach

Abstract: This paper applies real options analytic framework to firms' investment activity in information security technology and then a dynamic analysis of information security investment is explored by extending Gordon-Loeb (2002). The current research provides how firms have to respond to immediate or remote threat numerically. It shows that although positive drift of threat causes both larger and later investment expenditure, negative drift causes immediate investment and lower investment expenditure. The efficiency of vulnerability reduction technology encourages firms to invest earlier and induces cost reduction. To know the form of vulnerability is important because the effect of high vulnerability on timing and amount of the investment expenditure is mixed.

1. Introduction

Importance of information security has emerged very rapidly as information society has developed great deal. The information security investment has accordingly been considered by Gordon and Loeb in 2002. The highlight of their analysis is an introduction of vulnerability concept to formal optimization problem. Although Gordon-Loeb (2002) mentioned aspects of dynamics such as a first-mover advantage or the time value of money, their analysis is static and they did not consider any aspect of dynamic theory of information security at all. A dynamic analysis of information security investment is therefore explored in the following of this paper, in terms of real options theory often used for the analytic tools of investment timing.

The paper is organized as follows. First, Section 2 presents an outline of Gordon-Loeb model. Next in Section 3 we introduce real options theory that achieves the optimal timing of the investment level. In Section 4, we numerically calculate the optimal investment timing and level, additionally some comparative statics. Then finally, Section 5 draws some conclusions and mentions directions for future works. We point out necessary extension of the model which captures an equilibrium nature of information security investments and needs to estimate the parameters of the dynamics.

2. Optimum Investment Size: The Model of Gordon and Loeb

In order to estimate the optimal level of information security investment for protecting some information system within a firm or an organization, Gordon-Loeb (2002) considers several variables and parameters of the system. We will utilize similar notation with a little change only for expositional purpose.

First, let L denote the potential loss associated with the threat against the information system, i.e. $L = T\lambda$, where T is a random variable of the threat occurring and λ is the (monetary) loss suffered on conditioned on the breach occurring. Further, let v denote vulnerability, i.e. the success probability of the attack once launched; vL is then the total expected loss associated with the threat against the information system.

If a firm invests z dollars in security, the **remaining vulnerability** will be denoted by $S(z, v)$. The expected benefit from the investment which is the reduction in the expected loss attributable to the investment can then be computed as $(v - S(z, v))L$, where $(v - S(z, v))$ is the reduction in the vulnerability of the information system. The expected net benefit can therefore be computed as $(v - S(z, v))L - z$. Under suitable differentiability assumptions (see the conditions A1- A3 below), we can see that the optimal level of investment can be found by computing the local optimum z^* of the expected net benefit, i.e. by solving the first order equation:

$$\partial[(v - S(z, v))L - z]/\partial z = 0$$

and obtaining the following condition for $z^* = z^*(v)$:

$$-\partial S(z^*, v)L/\partial z = 1, \qquad (1)$$

Of course, the remaining vulnerability function can not be arbitrary. Since $S(z, v)$ could be interpreted to be a probability, we must clearly have $0 \leq S(z, v) \leq 1$. Its first argument is an investment and the second one another probability, so that $0 \leq z$ and $0 \leq v \leq 1$. Besides that, the following restrictions are defined in Gordon-Loeb (2002):

A1. $\forall z$, $S(z, 0) = 0$, i.e. if the attack success probability is 0, it stays so after every possible investment.

A2. $\forall v$, $S(0, v) = v$, i.e. if we spend no money for investment, there will be no change in the attack success probability.

A3. The function $S(z, v)$ is continuously twice differentiable and for $0 < v$: $\partial S(z, v)/\partial z < 0$ and $\partial^2 S(z, v)/\partial z^2 > 0$. Additionally, $\forall v$, $\lim_{z\to\infty} S(z, v) = 0$.

The condition A3 is asserting that with increasing investments it is possible to decrease the vulnerability level, but at a decreasing rate. Nevertheless, investing larger and larger amounts it is possible to make the attack probability arbitrarily small.

In their paper, Gordon and Loeb give two examples of function families that satisfy the conditions A1-A3 [1], namely:

$S^{I}=v/(\alpha z+1)^{\gamma}$, $(\alpha>0, \gamma \in R)$ and $S^{II}=v^{\alpha z+1}$, $(\alpha>0)$.

There are several characteristics in Gordon-Loeb (2002). Applying the first order condition (1) we can find the optimal level of investments $z^*(v)$. It is a natural idea to compare the optimal investment level to the total expected loss vL. Although it is proved that $z^*(v) < vL$ for all functions $S(z, v)$ satisfying the conditions A1-A3 and even more that $z^*(v) < (1/e)vL$, where $(1/e)$ is a constant, security investment z may be or may not be greater than loss λ in Gordon-Loeb (2002).

It is another characteristic of Gordon-Loeb (2002) that the vulnerability v, the remaining vulnerability $S(z, v)$ and the loss λ are independent of the value of the information system defended against attack.

3. Optimal Timing of Information Security Investment

3-1. Dynamic Considerations

The analysis by Gordon-Loeb (2002) is often referenced, very important and very fundamental. However in their framework the effect of investment does not affect future security of the information system although they mention it as "investment". With the model we could not analyze the timing of the investment. After all we could understand they are not dealing with "investment". Optimal starting time problem which is one facet of investment, is therefore explored in the following, using real options theory in order to know dynamic aspect of information security investment.

In reality, information security management often has considerable flexibility on when to enter or exit an investment project, and on the scale of the initial and subsequent commitments to make to the project. The firm's option to abandon a project during its life amounts to a put option on the remaining cash flows associated with the project. Ignoring the value of these options as done in standard discounted cash flow techniques can lead to incorrect investment evaluation decisions. The value of this flexibility is best captured by real options analysis, the application of option pricing techniques to capital budgeting. It has been established more than a decade ago

(Pindyck (1991), Dixit-Pindyck (1994), Trigeorgis (1996) and also Copeland-Antikarnov (2001) for example) that real options are crucially important in project evaluation.

The value of the option to postpone or delay the new activity (or discontinuing the old activity) becomes a value added which the decision could create, although it must bear cost. The value added could be calculated as a function of the value of the information system.

Traditional cost minimization technique like Gordon-Loeb (2002) systematically undervalues most investments. Real options analysis allows us to arrive at more accurate valuations of managerial flexibility or strategic value for information security that facilitate better investment decisions than we would arrive at using standard cost minimization analysis.

3-2. Literature Review

Using a real options model, this paper addresses two fundamental questions in the economics of information security area: (1) "How much to invest in information security" and (2) "When to invest?". Although several articles which deal with real options and information security address the issue: for example, Gordon-Loeb-Lucyshyn (2003), roundtable discussion on options and security presented at the second WEIS 2003 and Herath-Herath (2009), this paper represents one of the first attempts at analytically modeling continuous real options applied to information security.

As a capital budgeting technique for evaluating any projects, a real options approach is known to be promising. It is thus very natural to apply it to information security projects.

Gordon-Loeb-Lucyshyn (2003) introduces a discrete tree model of real options into the security literature for manager/practitioner focus. However a formal model is not developed and neither the optimal solution is considered. Herath-Harath (2009) introduces also a discrete tree model of real options with an additional feature of Bayesian postaudit from the management point of view.

Continuous real options model is different from either financial options or discrete tree model of real options. Real options have more flexible feature than financial options as Trigeorgis (1996) and others emphasize. The discrete tree model of real options has such a definite advantage as visibly showing the underlying mechanism. It is also very easy to understand and calculate solutions in a simple example. Although it provides good exhibition or classroom materials, its complexity explodes and it becomes very hard to derive the solution once applied to the complicated real world.

Discrete tree model could not deal with infinite horizon optimization problem. Since firm is a

typical infinite entity as a going concern (at least intends to be so), this defect is crucial when we are treating optimization problems which firm faces. Discrete tree model could not be solved analytically, only be solved by numerical analysis. Error by its approximation enters inevitably in numerical analysis and accumulates when we calculate solutions of long distant future. This causes troubles in risk management.

It is true that both continuous model and discrete tree model are needed, but there are actually no works on building continuous real options model applied to information security investment. These considerations make clear the contribution of our paper beyond the preceding literatures.

It would be always very nice to see how well modeling fits real data. Our concern is not only purely theoretical that how it is formulated theoretically, but also to see how well this fits real data. We set realistic and plausible parameter values to see how the model works in the real world.

3-3. Formulation and Solution

In order to give an example of suitable dynamic decision by a firm with optimal starting time for information security investment, we extend the model of Gordon-Loeb.

First of all we let the threat of attempted breach T_t follows geometric Brownian motion with drift

$$dT_t = \mu T_t dt + \sigma T_t dw \qquad (2)$$

where the subscript t is the time of calculation, dw is the increment of the Weiner process, μ is a drift parameter and σ is the volatility of the process. We denote the initial value of the threat $T_0 = T$ (unsubscripted capital letter).

The drift parameter μ could be negative although the volatility σ of the process has to be positive. Gordon-Loeb (2002) considers T_t as the probability rather than a random variate and confined it to [0, 1]. We do not need to stick to this assumption.

We assume further, letting the risk free interest rate r that

$$(r - \mu) > 0 \qquad (3)$$

for the existence of the maximization, avoiding the explosion of the maximand.

The present value of the expected benefit from the investment for the whole life after at the time of τ security action will be taken is:

$$\int_{\tau}^{\infty} e^{-rt} \{(v - S(z,v))\lambda T_t - z\} dt \qquad (4)$$

The present value discounted at the risk free interest rate r for the whole life is just the value of the system once an investment is determined at the time of τ. Since z is zero and $S(0, v)$ is v until the

time of τ because of A2, the maximand until the time of τ is therefore zero. Thus the general formula for the total expected benefit value of the system is given by equation (4), which firms try to maximize[2].

We assume that v and λ are independent of time and security investment is taken place only once at the time of τ. $S(z, v)$ is therefore independent of time. The maximized value $V(T)$ then becomes:

$$\begin{aligned} & V(T) \\ & = \sup_{\tau \in \Im} E[\int_{\tau}^{\infty} e^{-rt} \{(v - S(z,v))\lambda T_t - z\} dt] \\ & = \sup_{\tau \in \Im} E[e^{-r\tau} \int_{\tau}^{\infty} e^{-r(t-\tau)} \{(v - S(z,v))\lambda T_t - z\} dt] \\ & = \sup_{\tau \in \Im} E[e^{-r\tau} (\frac{(v - S(z,v))\lambda T_t}{r - \mu} - \frac{z}{r})] \end{aligned} \tag{5}$$

The derivation of last equation in (5) can be done similarly to that in Pindyck (1991). Thus we obtain the following solution. The value of an infinite option must satisfy an ordinary differential equation (ODE)

$$\frac{1}{2}\sigma^2 T^2 V^2(T) + \mu T V(T) - rV(T) + (v - S(z,v))\lambda T - z = 0$$

which can be solved analytically, and a solution to the second order ordinary differential equation can be found by testing a power solution of the form:

$$V(T) = \begin{cases} A_1 T^{\beta_1} + A_2 T^{\beta_2} & for \;\; T \le T^* \quad (6) \\ \dfrac{(v - S(z,v))\lambda T}{r - \mu} - \dfrac{z}{r} & for \;\; T \ge T^* \quad (7) \end{cases}$$

where $\beta_1 > 1$ and $\beta_2 < 0$ are the roots of the characteristic equation:

$$\frac{1}{2}\sigma^2 \beta^2 + \left(\mu - \frac{1}{2}\sigma^2\right)\beta - r = 0 \tag{8}$$

The following boundary conditions at the optimal time of making the decision:

$$\lim_{T \to 0} V(T) = 0 \tag{9}$$

$$A_1 (T^*)^{\beta_1} = \frac{(v - S(z,v))\lambda T^*}{r - \mu} - \frac{z}{r} \tag{10}$$

$$\beta_1 A_1 (T^*)^{\beta_1 - 1} = \frac{(v - S(z,v))\lambda}{r - \mu} \tag{11}$$

Equation (9) is called as "no-bubble condition" which prevents the divergence of the value function when $T = 0$, that is, there are no value without potential threats. Equation (10) is the "value-matching condition" which states that equations (6) and (7) become equal at T^*. Equation (11) is the "smooth-pasting condition" that states tangencies of both equations are equal. The above three conditions define the parameter A_1, A_2 and T^*:

$$A_1 = \left(\frac{(v - S(z,v))\lambda T^*}{r - \mu} - \frac{z}{r} \right) \left(\frac{1}{T^*} \right)^{\beta_1} \tag{12}$$

$$A_2 = 0 \tag{13}$$

$$T^* = \frac{\beta_1}{\beta_1 - 1} \left(\frac{r - \mu}{(v - S(z,v))\lambda} \right) \frac{z}{r} \tag{14}$$

Equation (12) follows from equation (10) directly, that is, solving equation (10) for A_1. Equation (13) is immediately derived from equation (9). Equation (11) together with equation (12) yields equation (14). Then the value function becomes:

$$V(T) = \begin{cases} \left(\frac{(v - S(z,v))\lambda T^*}{r - \mu} - \frac{z}{r} \right) \left(\frac{T}{T^*} \right)^{\beta_1} & for\ T \le T^* \quad (15) \\ \frac{(v - S(z,v))\lambda T}{r - \mu} - \frac{z}{r} & for\ T \ge T^* \quad (16) \end{cases}$$

which is dependent on the initial value of potential threat T.

This model is based on the real options theory (Pindyck (1991), Dixit-Pindyck (1994) and Trigeorgis (1996)) . Formally speaking it is rather orthodox. The increment d$V(T)$ increases as T increases where T is smaller than T^* as seen from equation (15). Then it stays constant as T becomes larger than T^* because $\partial V(T)/\partial T = (v - S(z, v))\,\lambda /(r - \mu)$. The maximization of $V(T)$ is therefore attained at T^*. In order to further detect the behavior of the value function $V(T)$, we define NPV (net present value) as the present value of the expected benefit from immediate investment, which is given by substituting $\tau = 0$ to equation (4). Consequently, the formula of NPV is given by equation (7) or (16). The difference of ($V(T)$ – NPV) is the value of waiting to invest.

Next, we find the optimal level of investments z*. It is attained by maximizing the expected benefit from the investment at T^*:

$$z(T^*) = \text{argmax}_{z \in R}\, V(T^*; z). \tag{17}$$

Note that the optimal level of investments depends on T^*. Because T^* also depends on z, the realized optimal level of investments must satisfy

$$z^* = z\left(\frac{\beta_1}{\beta_1 - 1}\frac{r-\mu}{(v - S(z^*, v))\lambda}\frac{z^*}{r}\right). \quad (18)$$

This expression, from equation (14), might not cause confusion. Finally, equation (17) means maximization of equation (16) , so we have the first order condition for z*:

$$-\partial S(z^*, v)\lambda T^*/\partial z = (r-\mu)/r, \quad (19)$$

which is the same as Gordon-Loeb's deterministic case if $\mu = 0$.

3-4. Interpretation

It is an economic problem whether firm should start information security investment today or later. The decision depends on the functional form of the **remaining vulnerability** S and also the properties of Brownian motion of the treat T_t. For example, facing negative trend of the threat (negative drift parameter μ) the firm may have inclined to postpone the investment. The value of the firm is furthermore considered dependent on the volatility of the process σ.

It is a natural interpretation in real options literature that if T_t becomes greater than T^* while watching the process of T_t, firm ought to invest in information security technology. For larger T^*, therefore, the investment timing becomes later because the firm must wait to investment until T_t reaches the larger value of T^*. On the other hand, the timing is sooner for smaller T^*. This T^* is called as optimal investment thresholds.

The $V(T)$ function is nonlinear in that it has a kink at T^*. The shape is dependent on r, μ, σ, λ, and v. Then we have to economically interpret the dependency, which will be done in the next section.

4. The Optimal Solution: Numerical Illustrations

In this section we numerically calculate the optimal investment thresholds T^* and the optimal level of investments z*. To perform the calculation, we use $S^{I}=v/(\alpha z + 1)^{\gamma}$, ($\alpha > 0, \gamma \in R$) and $S^{II}= v^{\alpha z+1}$, ($\alpha > 0$) for the remaining vulnerability function case I and II. Furthermore, we present a comparative statics analysis of the threshold and level of investments by changing parameters: volatility σ, drift μ, vulnerability v and the parameter of remaining vulnerability function α. Since the volatility σ represents the degree of uncertainty, among these it is the most important parameter in a real options model.

The drift μ represents the expected growth rate of the potential loss. The vulnerability v is interpreted to represent the urgency of information security investment. The parameter α is

interpreted to represent the **efficiency** of the investment. Since these parameters are important, we focus these parameters in this section. We assume that the hypothetical base values of the parameters are as follows: $\sigma = 0.2$, $\mu = 0.02$, $r = 0.05$, $v = 0.5$, $\lambda = 1$, $\alpha = 1$ and $\gamma = 1$. **Figure 1** shows the difference of the efficiency of vulnerability reduction between case I and II.

4-1. Remaining Vulnerability Case I

In this case, we use $S^{\mathrm{I}}=v/(\alpha z + 1)^{\gamma}$, ($\alpha > 0$, $\gamma \in \mathrm{R}$). By solving the first order condition after insertion of the function into equation (19),

$$-\frac{\partial}{\partial z}\left(\frac{v\lambda T^{*}}{(\alpha z+1)^{\gamma}}\right)=\frac{r-\mu}{r} \qquad (20),$$

we have

$$z^{*}=\frac{(\frac{r}{r-\mu}v\gamma\alpha\lambda T^{*})^{1/(\gamma+1)}-1}{\alpha}, \qquad (21)$$

which is the same as Gordon-Loeb's deterministic case if $\mu = 0$. Then, we have $T^* = 8.89$ and $z^* = 1.72$, under the hypothetical base values of the parameters. That is, suppose the potential loss reach \$8.89 (million) at the time of τ, the firm should start information security investment \$1.72 (million). After the investment, the remaining vulnerability will be reduced to 0.184 from the hypothetical vulnerability value 0.5.

Figure 2 displays the value functions and the net present value (NPV). The value function $V(T)$ is a convex function and tangent to the NPV at $T^* = 8.89$. This shape resembles the payoff of an American call option before the maturity. For $T < T^*$, the firm wait to investment because the value of waiting ($V(T)$ − NPV) is positive. For $T^* \leq T$, the value of waiting is 0, so that $V(T)$ coincides with the NPV. It shows an orthodox shape in a real options model.

Figures 3-6 display the comparative statics of the optimal investment threshold T^* and the optimal level of investments z^* with respect to σ, μ, v and α respectively. In **figure 3**, T^* and z^* are displayed with respect to σ. The relationship between T^* and σ is the same as that often observed in a real options model, which is high uncertainty leads to a high threshold, i.e., delay in investment. This is because the value of delaying investment increases in order to wait for new information under high uncertainty. On the other hand, we could see for z^* that high uncertainty σ requires larger amount of the investment expenditure.

In **figure 4**, we must distinguish the range of $\mu < 0$ from $\mu > 0$. For $\mu > 0$, high drift causes larger amount of the investment expenditure z^*, and hence forces the firm later investment. On the other hand, for $\mu < 0$, T^* is slightly decreasing with μ. There is a possibility that the expected

potential loss will decrease in the future. This implies that high negative drift makes the necessity of information security investment low. Hence, high negative drift causes later investment and lower investment expenditure. The consideration shows that our dynamic modeling of information security investment is properly formulated and yields reasonable conclusion.

In **figure 5**, we find an unique property that the vulnerability has no impact on the level of investments z* but the investment threshold *T**. Because of the emergency, high vulnerability requires immediate investment. However, the required expenditure is not a variant, independently of the vulnerability. Important thing in this situation is timing, not amount.

Figure 6, where *T** and z* are displayed with respect to α, shows interestingly enough that high efficiency of vulnerability reduction α encourages the firm to invest earlier and induces cost reduction.

4-2. Remaining Vulnerability Case II

In this case, we use $S^{II} = v^{\alpha z+1}$, ($\alpha > 0$). By solving the first order condition again after insertion of the function into equation (19), we have

$$z^* = \frac{\ln \frac{r-\mu}{r} - \ln(-\alpha v \lambda T^* \ln v)}{\alpha \ln v}, \qquad (22)$$

which is also the same as Gordon-Loeb's deterministic case if $\mu = 0$. Then, we have *T** = 9.99, z* = 2.53 and *S*(z*,*v*) = 0.087. Comparing with case I, the firm needs more expenditure and later investment due to more efficient reduction of vulnerability as shown above in **figure 1**.

Figures 7-10 display the comparative statics of the optimal investment threshold *T** and the optimal level of investments z* with respect to σ, μ, *v* and α, respectively. While **figures 7, 8 and 10** show the same property as in case I (in **figure 8**, the characteristic is more clearly), we can find a following interesting property in **figure 9**, from which we could say that case II has more natural result than case I.

Unlike in case I shown in **figure 5**, high vulnerability requires high investment expenditure in **figure 9**. This is due to the difference of the remaining vulnerability function in both cases. Furthermore, high vulnerability should require later investment, since *T** in **figure 9** is U-shaped with respect to *v*. High vulnerability requires high expenditure and later investment.

5. Concluding Remarks

5-1. Summary

It is intuitively true that firms have to respond quickly (very slowly) to immediate (remote) threat. We do not know how firms respond in the intermediate case. The current rigorous research provides the solution.

Positive drift of threat causes both larger amount of investment expenditure z* and later investment, while high negative drift causes immediate investment in spite of smaller amount of investment expenditure (**figure 4 and also figure 8**). The efficiency of vulnerability reduction technology encourages firm to invest earlier and induces cost reduction (**figure 6 and also figure 10**). High vulnerability requires either immediate investment independently of the amount of investment expenditure (**figure 5**) or delayed and larger amount of investment (**figure 9**).

It has been seen in the last section that case I and case II yield different results although their functional forms look alike as shown in **figure 1**. We do not know which function is valid in the real world. It would be therefore concluded that the estimation of $S(z, v)$ is very important especially in the sight of high vulnerability.

5-2. Remaining Problems

Several remaining problems are explored in the following.

(1) Dynamics Formulation

The investment expenditure z and therefore the vulnerability v could vary every period of time. Attackers come every moment from all over the world and with newer technologies armed. Defenders need to continuously execute information security investment in order to avoid defeated by the unrelenting attacks. Using dynamic control theory the optimal policy over time could be derived under the circumstance.

Furthermore a difficult problem remains left. Attackers strike suddenly. This might be described by a jump process of the threat. The forecasting of their arrival is not possible and any definite countermeasure could be hardly taken before attacks. The formulation of these phenomena will be our works to do next.

(2) Attackers' Behavior Formulation

It is also necessary to take some initial steps toward a better understanding of not only how firms invest in information security technology, but also how firms are faced with the threat (menace) of breach. To formulate attacker's behavior, we have to know what attackers are maximizing.

Attackers might threaten a firm to make an assault on the information system of the firm unless the firm pays money. Another objective of attackers might get the value of targeted firm.

They try to lose the confidence of customers or affect reputation of the targeted firm by causing disorder or being mixed up. They do anything to injure the credit of the targeted firm and to rob of their customers. However there is no guarantee to succeed their attempt. It is also possible that he or she is a criminal who enjoys watching how people/firm react to what he or she has done.

If the attack continues for long time, the defender takes action. Firm would defend themselves against the violent attack. Then the payoff of the attacker will diminish and the attacker will change their strategy. This long run problem is certainly hard to be captured.

Hence it is one of the toughest tasks to formulate attacker's objective function. Once we could formulate the attacker's behavior, the equilibrium becomes the solution to a complex 2-player problem. This would not be zero sum 2 person game, some of which could be easily solved by mathematical programming. If we could solve this problem by mathematical programming, however, it has a practical use and helps firms greatly.

(3) Empirical Analysis

We have to carry out empirical analysis by finding data of the threat and also vulnerability, and also estimating the distribution parameters of the probability of the threat and success probability of the attack. It would help understanding the real phenomena and constructing strategies of firms to know the parameter values.

As far as the mean and variability of the probability of the threat, we can rely on tools which have been developed in finance field. Having a strong foothold in finance, we could move the estimation forward. Once we know the character of the distribution, we could go back to the theory again and might be able to build a new theory with observations.

FOOTNOTES

1) Willemson (2006) postulated A3 slight differently and obtained other functional form, which state that $S(z, v) = 0$ if z is greater than a certain amount.

2) A typical real options problem is the model where the value of a firm once the capital stock K is determined is just the present value added of S (like M&A synergy) to K in the sacrifice of paying a cost f at the time of τ, discounted at the risk free interest rate. The general formula for the optimal timing problem with the value-added S obtained in the sacrifice of paying cost of f is given by:

$$\int_0^{\tau} e^{-rt} K x_t dt + \int_{\tau}^{\infty} e^{-rt} \{(K+S)x_t - f\} dt$$

where x_t is the return on capital.

If we define $S(z, v)$ and v differently, the model in the text has very similar solutions to this problem.

REFERENCES

Copeland, T., & Antikarnov, V., (2001), *Real options: A practitioner's guide*, Texere.

Dixit, A. K. and Pindyck, R. S., (1994), *Investment Under Uncertainty*, Princeton University Press.

Gordon L., A, and Loeb, M. P., (2002), "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, Vol. 5, No. 4, pp. 438-457.

Gordon, L., Loeb, M., and Lucyshyn, W., (2003), "Information security expenditures and real options: a wait- and-see approach," *Computer Security Journal*, 19(2), pp. 1-7.

Gal-Or, E. and Ghose, A., (2005), "The Economic Incentives for Sharing Security Information," *Information System Research*, pp.186-208. (http://129.3.20.41/eps/io/papers/0503/0503004.pdf)

Herath, H., and Harath, T., (2009), "Investments in Information Security: A Real Options Perspective with Bayesian Postaudit," *Journal of Management Information Systems*, Winter, Vol. 25, No. 3, pp. 337-375.

Pindyck, R. S., (1991) "Irreversibility, Uncertainty, and Investment," *Journal of Economic Literature*, 29, 3, September, pp. 1110-1148.

Roundtable discussion in WEIS 2003 (see http://www.cpppe.umd.edu/rhsmith3/agenda.htm).

Trigeorgis, L. (1996), *Real Options*, MIT Press.

Willemson, J., (2006), "On the Gordon & Loeb Model for Information Security Investment," The Fifth Annual Workshop on Economics and Information Security (WEIS06).

FIGURES

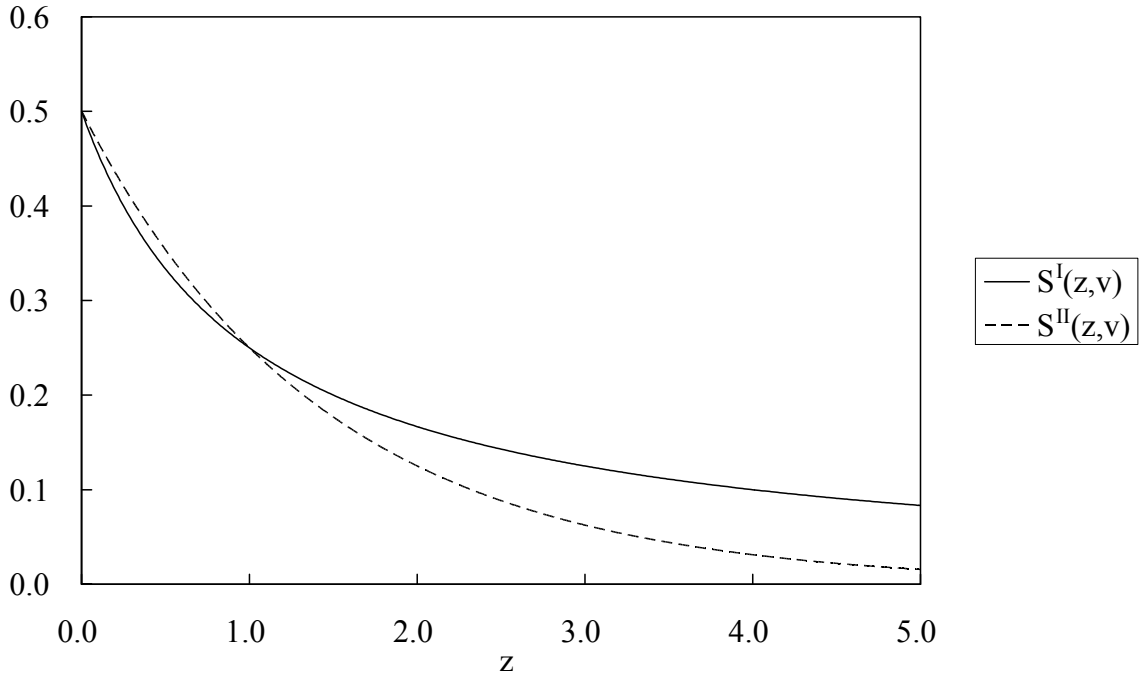

Figure 1: The remaining vulnerability function in case I (solid line) and II (dashed line).

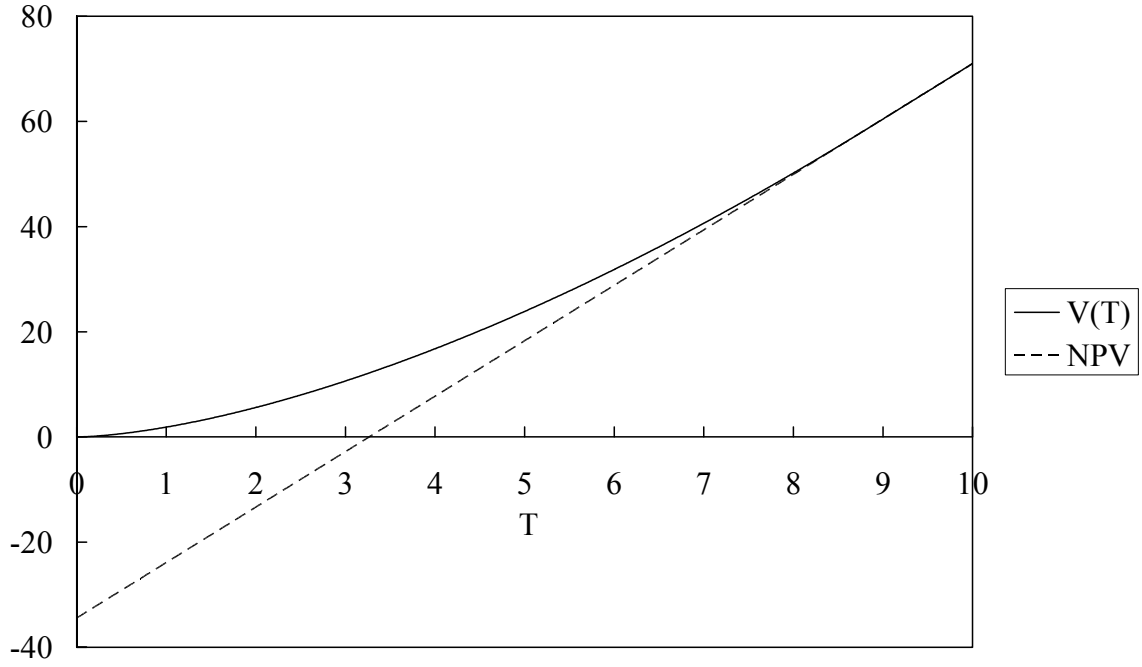

Figure 2: The value function *V*(*T*) (solid line) and NPV (dashed line) in case I.

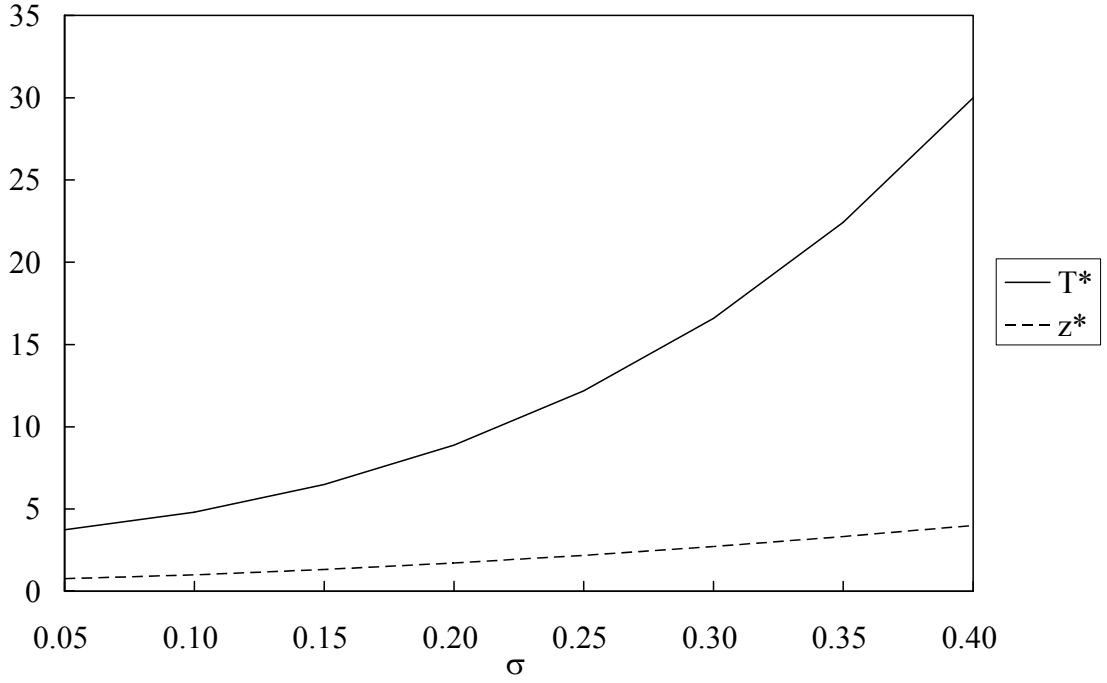

Figure 3: The comparative statics of the optimal investment threshold *T (solid line) and the optimal level of investments z* (dashed line) with respect to σ in case I.**

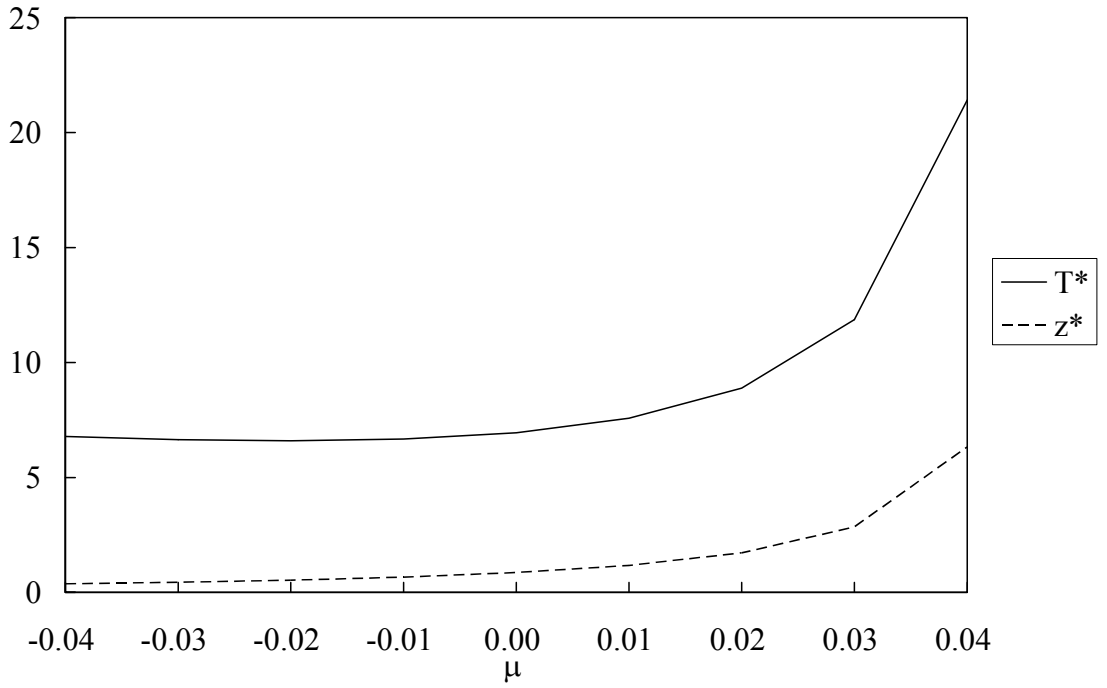

Figure 4: The comparative statics of the optimal investment threshold *T (solid line) and the optimal level of investments z* (dashed line) with respect to μ in case I.**

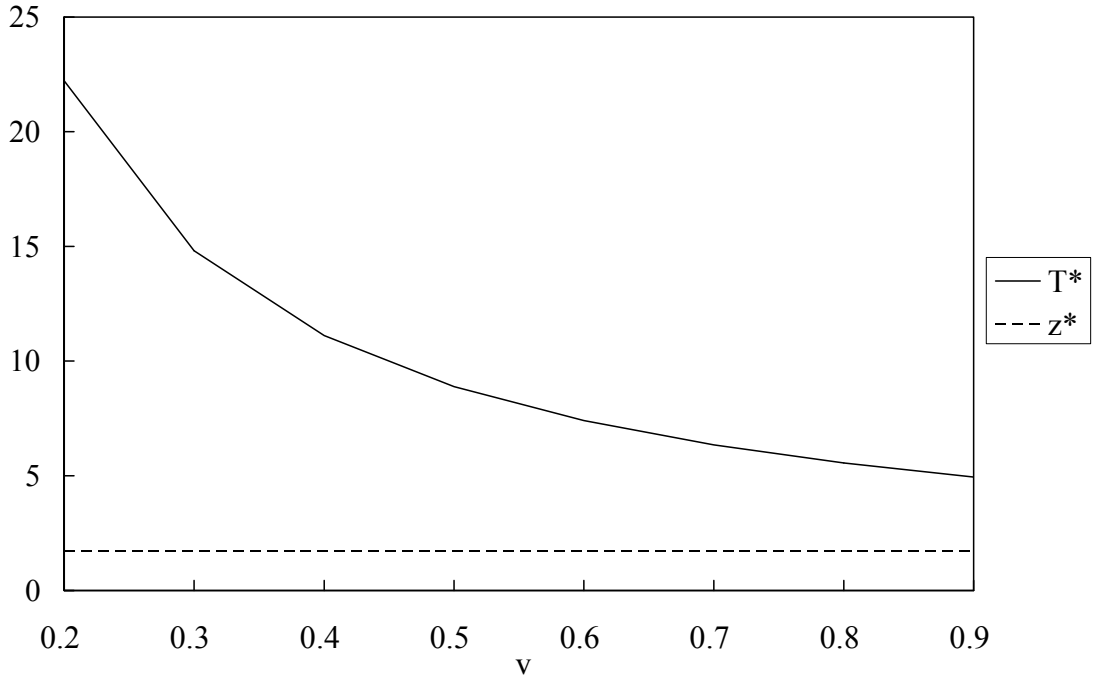

Figure 5: The comparative statics of the optimal investment threshold *T (solid line) and the optimal level of investments z* (dashed line) with respect to *v* in case I.**

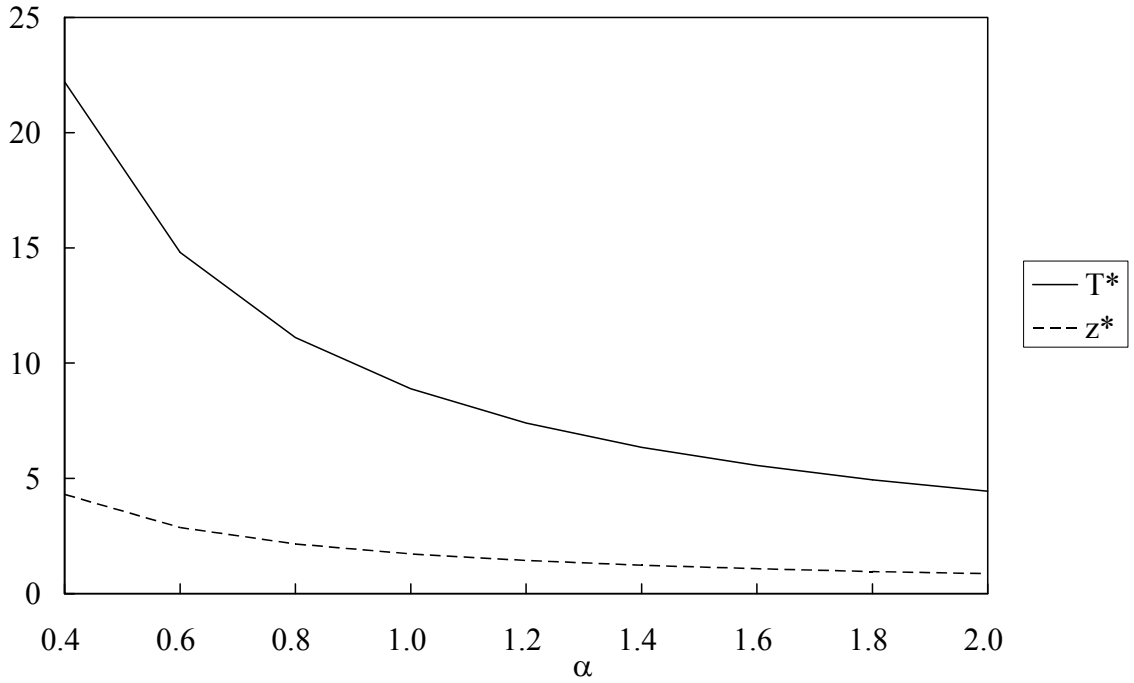

Figure 6: The comparative statics of the optimal investment threshold *T (solid line) and the optimal level of investments z* (dashed line) with respect to α in case I.**

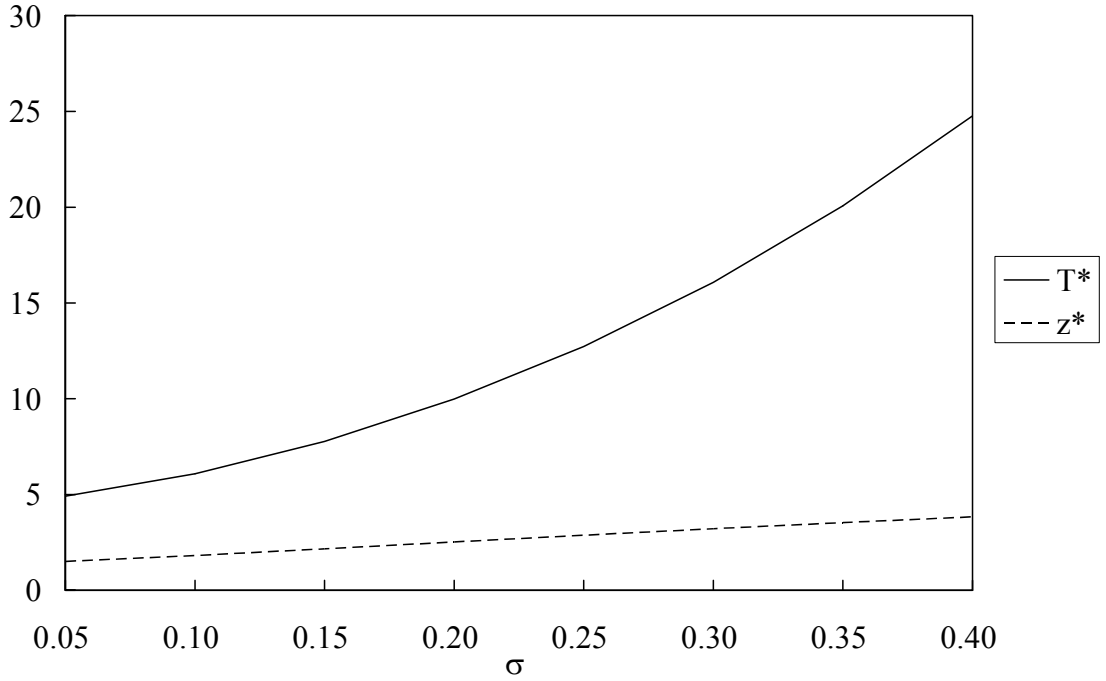

Figure 7: The comparative statics of the optimal investment threshold *T (solid line) and the optimal level of investments z* (dashed line) with respect to σ in case II.**

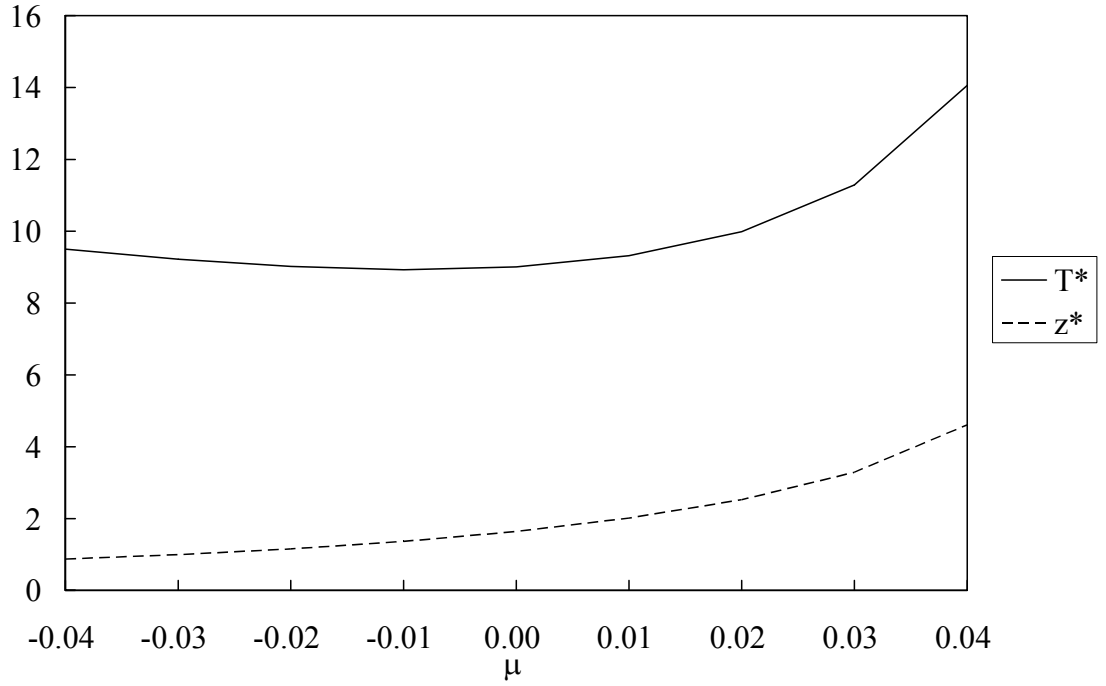

Figure 8: The comparative statics of the optimal investment threshold *T (solid line) and the optimal level of investments z* (dashed line) with respect to μ in case II.**

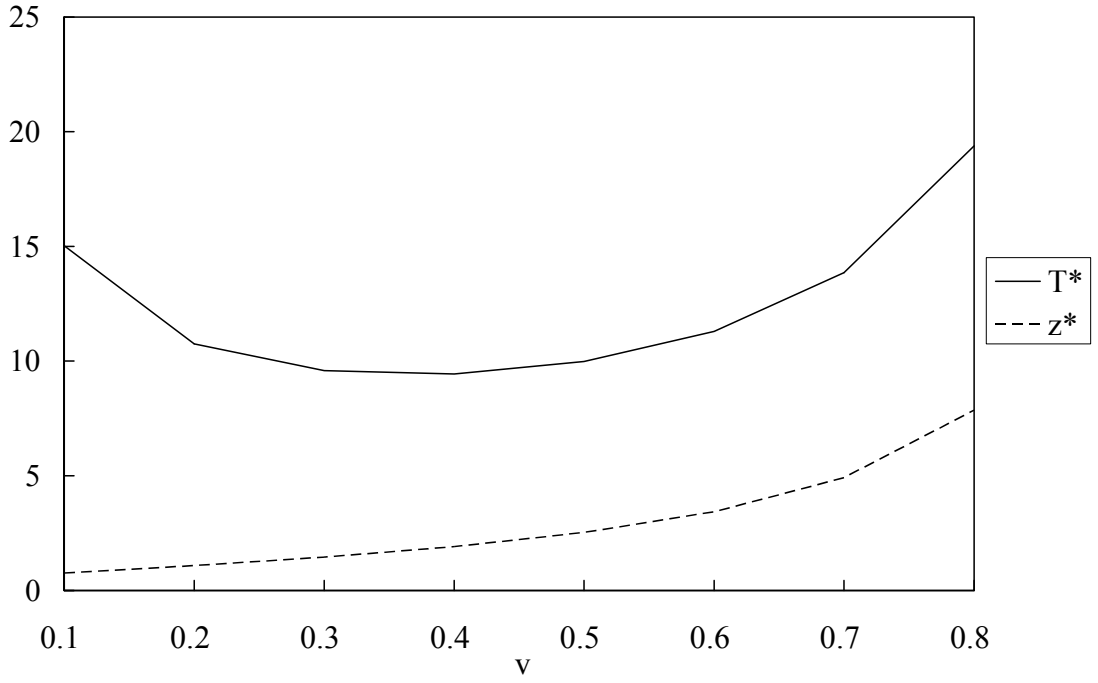

Figure 9: The comparative statics of the optimal investment threshold *T (solid line) and the optimal level of investments z* (dashed line) with respect to *v* in case II.**

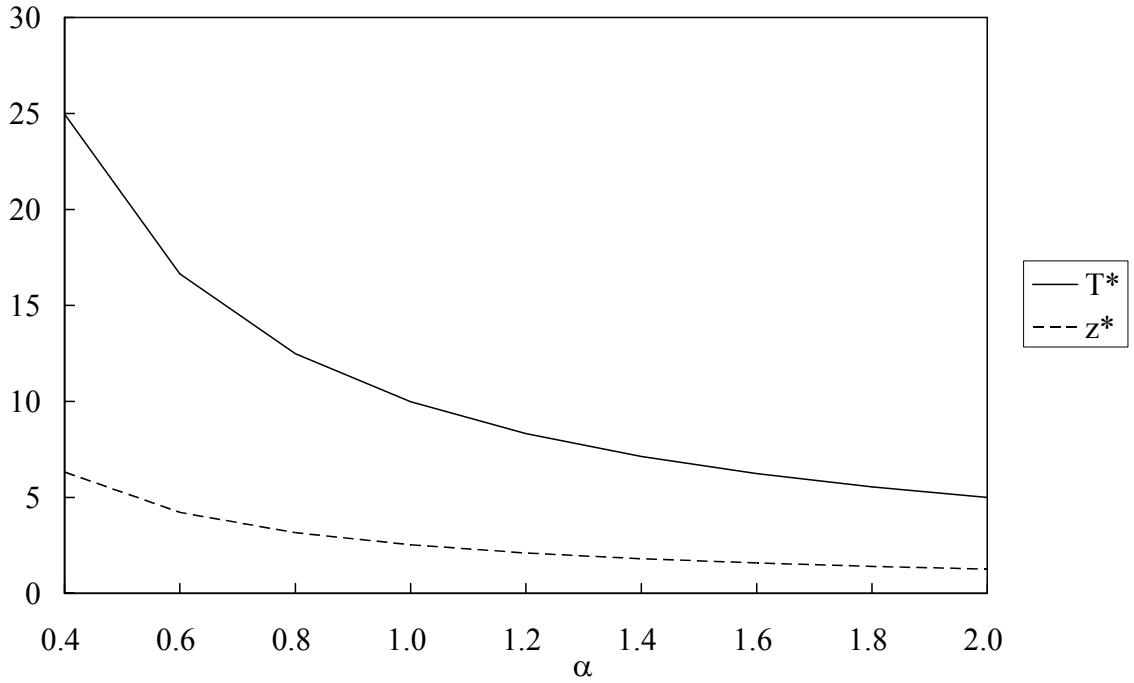

Figure 10: The comparative statics of the optimal investment threshold *T (solid line) and the optimal level of investments z* (dashed line) with respect to α in case II.**