Discussion Paper, Series A, No.2016-303

Rational Theory of Information Security Battle: Economic Analysis of Preemptive Behavior

Makoto Goto and Ken-ichi Tatsumi

June.2016

Graduate School of Economics &
Business Administration
Hokkaido University
Kita 9 Nishi 7, Kita-Ku, Sapporo 060-0809, JAPAN

Rational Theory of Information Security Battle: Economic Analysis of Preemptive Behavior

Makoto GOTO
Graduate School of Economics and Business Administration,
Hokkaido University, Kita 9, Nishi 7, Kita-ku, Sapporo 060-0809, Japan
E-mail: goto@econ.hokudai.ac.jp

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

February 22, 2013
June 28, 2016 (This version)

Keywords: information security investment; preemptive behavior; threat; optimal timing; real options theory
JEL(s): D24, D81, E22, L86, M15.

Abstract: We develop a model of a zero-sum information security game by introducing a reward function (called *P*-function) for cyber attackers into the models of Gordon and Leob (2002) and Tatsumi and Goto (2010). Then the preemptive behavior of cyber attackers or defenders is analyzed. The derivation of the optimal behavior is based on a real options theory and the properties are numerically calculated.

Through our numerical analysis cyber attackers are turned out to be rational in the sense that they are very sensitive and quickly respond to both the monetary gain that they will obtain and the vulnerability of defenders. We further observe among others that, in many cases, defenders can optimally preempt. However, this is because attackers have no incentive to attack targets with a small monetary gain.

---

*) We are grateful to many individuals who provided us with valuable and helpful comments. All remaining errors are our own.

Rational Theory of Information Security Battle: Economic Analysis of Preemptive Behavior

Abstract: We develop a model of a zero-sum information security game by introducing a reward function (called *P*-function) for cyber attackers into the models of Gordon and Leob (2002) and Tatsumi and Goto (2010). Then the preemptive behavior of cyber attackers or defenders is analyzed. The derivation of the optimal behavior is based on a real options theory and the properties are numerically calculated.

Through our numerical analysis cyber attackers are turned out to be rational in the sense that they are very sensitive and quickly respond to both the monetary gain that they will obtain and the vulnerability of defenders. We further observe among others that, in many cases, defenders can optimally preempt. However, this is because attackers have no incentive to attack targets with a small monetary gain.

1 Introduction

Security breaches could occur almost every second. Thus the importance of information security has increased very rapidly as information technology has developed greatly and the information society has changed.

Although the majority of security incidents such as huge data theft reported over the last several years have involved stolen PCs or misplaced storage for example, there have also been incidents that reflect criminal attempts to steal valuable corporate information. Cyber attackers have sought to pull off such crimes.

Recent incidents illustrate the trend of attackers gearing toward profit-motivated cybercrimes. There is also a trend [1] of shifting from indiscriminate attacks to targeted attacks. Thus researchers consider it necessary to take steps toward better formulation of not only how firms invest in information security technology, but also how cyber attackers behave and how firms face their threat (menace) and respond to it.

Information security investment has been proposed by Gordon and Loeb (2002). The highlight of their analysis is the introduction of the vulnerability concept into the formal optimization problem. Because their analysis is static, Tatsumi and Goto (2010) explored a fundamental dynamic (optimal timing) analysis of information security investment from the defender's perspective.

In this study, we add the attacker's perspective to the security investment problem

and formulate the problem of both security and offensive investments as a two-player zero-sum game. Such a situation has never been considered before to the best of the authors' knowledge. The theory of the optimal timing of information security investment plays a crucial role in the present study as discussed below.

We analyze how cyber attackers behave under reasonable assumptions and highlight preemptive attack, one example of which is known as so-called the zero-day attack. We also analyze when and how defending firms execute preemptive defense towards such an attack.

This paper is organized as follows. First, Section 2 presents an outline of cyber attack and attackers under recent circumstances. Next, in Section 3, we introduce an attacker's behavior under a static setting and analyze the static equilibrium between an attacker and a defender. In Sections 4 and 5, we introduce a model of an attacker's behavior under a dynamic setting, using a real options theory that achieves the optimal timing of the investment level. Notions of preemptive attack and preemptive defense are explored in detail. Then, in Section 6, we numerically calculate the optimal investment timing and level, in addition to some comparative statics. We focus on the effect of key variables on preemptive behavior. Finally, in Section 7, we draw some conclusions and present directions of future works.

2 Attacker and Circumstances

2-1 Background

(1) Changing Circumstances

There are many security tools nowadays. Although behavior towards information security will vary among firms, the actual strategy for information security taken by firms is something like the following.

A firm realizes that facing security threat definitely need not use all security tools at the same time before the attack. The firm may choose only one or some of them, at a given time and also to some degree, if technologically possible, depending on cost and benefit analysis. Thus, there might be a timing order of installment or introduction for security tools. Corporate budget might force a firm to give up the installment of a specific security tool. Several technological reasons might also be behind its turn of installment for each information security tool [2]. A cyber attacker appears suddenly and the firm is forced to quickly finish the installment of a security tool.

Today any security investment incurs cost but its economic benefit, if any, arises only in the future. If no economic benefit is thought to arise and if any security investment is not executed, a dangerous situation will develop.

With time, relationships among variables might change, which means that circumstances (parameters of the model) will change and as well as the decision. The optimal decision under such circumstances will be either to execute or not to execute investment. Even when it is decided not to execute, a decision when to execute remains still. This is the optimal timing decision, which is solved by a real options theory.

(2) Asymmetries: Several Aspects

There are several specific asymmetries in the actual cyber-security battle between attackers and defenders. Defenders avoid losing something important by installing information security tools and therefore by investing the amount of investment required to protect their information. However, they will have neither immediate nor apparent gain from the money spent.

On the other hand, attackers are different. Attackers attack by investing in offensive tools or skills, but without risking possible loss of their own monetary value. This is because the party that loses either money or reputation is definitely the defender and the monetary value of the attackers is well-fortified. Attackers regret (not any apparent loss) withdrawal from or postponement of an attack. Thus, the behavioral objectives are quite different between attackers and defenders.

There is another situation that can be called reciprocal informational asymmetries. Nowadays, it is often observed that, after defenders have installed security tools, hackers attack specific parts by checking the vulnerabilities of the defenders and opportunistically intruding through the vulnerable part if any.

One example could be listed under reciprocal informational asymmetries. Attackers try to exploit vulnerabilities that are not yet known to others including the developer of the software or system. This is known as the zero-day (or zero-hour or day zero) attack or threat and occurs before the developer covers up the security hole to prevent attackers from carrying out an attack.

People might deem this game unfair. An unfair game, strictly speaking, is a game in which a certain player can always win even if he or she plays properly [3]. It seems attackers are unfair because they never lose, as explained above.

(3) Attackers and Their Behavior

Attackers try to access to computer networks with customers' personal data such as credit cards, debit cards, driver's license and check information. This network intrusion highlights the unending effort of criminals to target massive databases of consumer information. Such information is then sold to other parties for fraud and other crimes. The information stolen directly from computer databases is thus used in criminal activity.

Another purpose of stealing information might be to get the market position or

brand prestige of competing firms. Alternatively attackers might threaten a company to destroy the information system of the company unless it pays them money.

We now have good knowledge of how intruders do get access to information and also how long an intrusion goes undetected. However, we still do not know exactly the cost a firm actually incurs as a result of the intrusion.

However, it could be stated, at least, that defenders try to minimize vulnerabilities, thereby minimizing the cost for defenders. To maximize the gain for attackers is to maximize the remaining vulnerabilities. Thus attackers try to maximize the remaining vulnerabilities.

Although it is also reported that the main trend is a shift from an indiscriminate cyber attack to a targeted cyber attack, some attackers surely behave with irrational incentives, while others behave within limited resources and thus have to be rational. The latter, compared with the former, might have a notion of the cost/benefit to attack.

Although cyber attackers have been alternatively called as hackers, crackers, black hats or malware code writers, the term “economic predators” has recently emerged in light of the economic damage they cause. Their target is limited and their aim is to obtain valuable information held by targeted firms or to damage the reputation of targeted firms.

Targeted cyber attack has something to do with the value of the target. A target without any value is neither defended nor attacked. Security tools will help firms better protect themselves and their customers from attackers wanting to steal intellectual properties.

2-2 Principles and Assumptions

To formulate the attacker’s behavior just described briefly, we have to know what attackers are maximizing. Rational attackers will choose, as targets, firms with a defensive strength lower than the value that the attackers might want to steal or obtain by threatening. Defensive strength is thought as the remaining vulnerability in the economics of information security [since the work by Gordon and Loeb (2002)], although it is difficult to concretely specify and empirically measure defensive strength or ability.

Therefore, attackers will exploit the remaining vulnerability to plunder and obtain profit. Such penetration or plunder will be explored further and formulated in later sections. Other underlying assumptions are explored here as follows.

(1) Fairness Assumption

It surely is interesting to determine why the unfair game mentioned above happens and why attackers are unfair. However, to determine what happens if the reverse is true (attackers are fair) we assume the following fairness assumption:

Attackers do not know what types of information security tool are installed by defenders. Equally, defenders do not know what types of offensive tool are installed by attackers.

This underlying assumption might also be called a fair game assumption if we formulate it rigorously. It is only made to determine the fundamental relationship between attackers and defenders.

(2) Rational Attacker Assumption

The rationality of some attackers is easily justified with recourse to industrial cyber espionage. Spies could also be used to steal technology information and sabotage the defending enemy in various ways. Espionage or spying involves an individual or a group of individuals (an organization) obtaining information considered secret or confidential without the permission of the information holder. Such offense technology has shown remarkable improvement over those previously used. Attackers are also reported to effectively combine various technologies to attack. They are rational at all.

Since we know the story of industrial cyber espionage and the discussions in the previous and current subsections will provide more details, there is therefore no need to explain more on the subject [4] even if we assume the following:

Attackers are rational in the sense that they perform a cost/benefit analysis of the attack into account.

By no means are we saying that there is no irrationality in cyber attack. It is definite that larger firms generally have a good reputation and therefore are at higher risk of being attacked by hacktivism, which uses information networks as a means of protest to promote political ends. Rather, we assert that the rational theory of cyber attack becomes a starting point for determining irrational behavior.

An unexpected random behavior of cyber attack is caused partly by the geometric Brownian motion and defenders could not determine such behavior. This is another asymmetric nature of the model that follows.

(3) Common Knowledge Assumption

There are many kinds of cyber offensive technologies and their technical levels might be diverse, i.e., new or outdated, and high or low. We therefore assume that:

Even if attackers do not invest in offensive tools, they could attack using common knowledge of technology.

Even if there is no offensive investment ($y = 0$ in the later terminology in Section 3-1), therefore, the lack of defensive investment ($z = 0$ in the later terminology) is not necessarily optimum for defenders.

(4) Forgone Vulnerability Assumption and Diminishing Marginal Returns Assumption

Defenders do not know the destination of their forgone vulnerability. Attackers obtain such forgone vulnerability, the value of which is not necessarily the same as what defenders feel they have lost. The gain of attackers might be larger than the loss of defenders. We, however, assume the following:

What rational attackers obtain is proportional to the forgone vulnerability of targeted defenders.

Another assumption is made on the basis this assumption. Attackers start attacking targets with a higher payoff. If the attack continues persistently, the number of targets decreases. The payoff might be exhausted gradually. Therefore, the payoff for attackers will marginally diminish as offensive investment increases (**diminishing marginal returns assumption**). In Section 3-1(2) below, these assumptions are formulated rigorously as the *P*-function.

Accordingly, we could surmise that firms with valuable systems have to invest more to be better fortified. Furthermore, we have to add two points. If the attack continues persistently for a long time, defenders might take definitely action someday. Firms would definitely defend themselves against violent attack.

2-3 Other Miscellaneous Topics

(1) Multiple Agents' Problem

A game theoretic model between two firms both on the defensive side was built by Gordon-Loeb-Lucyshyn (2003). The model deals with the interaction between two defenders, contrary to the current model that follows. Two defenders are with and without information sharing, where each firm minimizes their expected information security cost - the expected cost due a breach plus the cost of information security investments.

It is shown then that at the (Nash) equilibrium, each firm spends no more (and often less) on information sharing than it does in the absence of sharing. In most cases, information sharing will increase the overall level of information security, i.e., the probability of a breach goes down. In all cases, information sharing increases social welfare (more security for less dollars). However, an interesting result is also shown that if the level of information sharing is endogenous, then each firm has incentives to a free ride and not to share.

(2) Value and Cost of Waiting to Invest

Some firms introduce new information security tools by committing the sunk cost up-front and immediately investing at full scale. The sunk cost means that there is no cyber attack and therefor the expenditure on the investment becomes a waste. Other firms start out more cautiously, for example, by first undertaking market research and then launching a pilot project. One of the indirect costs of such a strategy by firms is

that the decision on the cost of waiting to invest may reveal the firms themselves, bringing face to face with a sudden cyber attack.

Literature on the real options theory has provided new insights into managing irreversible capital investments whose payoffs are always uncertain. Two of the most important predictions from such a theory are as follows: (i) greater risk delays a firm's investment timing and (ii) greater risk increases the option value of waiting. Although the real options theory highlighted the value of waiting to invest [5], we will focus on the cost of waiting to invest. We will consider a situation in which some defending firms, while waiting, come across a preemptive attack.

3. Static Optimum Investment Size: Beyond the Model of Gordon and Loeb

The defender's problem is described first, following Gordon and Loeb (2002), and then the attacker's problem is formulated. After the decisions of both the defender and the attacker are explored, then the interaction between them is formulated in a static setting.

The situation is like bilateral monopoly [6] in a sense. There are two parties fighting each other. Both parties have conflicting goals, with the final situation settling in between the two sides' points of maximum benefit or profit.

3-1 Environment and Decision

(1) Defender's Environment and Decision: Model of Gordon and Loeb

To estimate the optimal amount of information security investment for protecting some information system within a firm or an organization, Gordon and Loeb (2002) considered several variables and parameters of the system. We will utilize a similar notation with a slight modification 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, the detail of which we will describe later and λ is the monetary loss suffered under the condition of breach occurring. Furthermore, let v denote the 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** is denoted by $S(z, v)$. The remaining vulnerability function cannot 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 and 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 for $0< v$: $\partial S(z, v)/\partial z < 0$ and $\partial^2 S(z, v)/\partial z^2 > 0$. Additionally, $\forall v$, $\lim_{z\to\infty} S(z, v) = 0$.

Condition A3 asserts that, with increasing investment, it is possible to decrease vulnerability, but at a decreasing rate. Nevertheless, by investing more it is possible to make the attack probability arbitrarily small.

In their paper, Gordon and Loeb give two examples (cases I and II) of function families that satisfy conditions A1-A3, namely,

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

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

It is another characteristic of Gordon and 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 an attack.

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

(2) Attacker's Environment and Decision

We next analyze a rational attacker whose behavior is described in the previous sections. What the rational attacker will obtain is assumed to be proportional to the expected loss of the information of a targeted firm. It is called the monetary loss parameter in the previous subsection. Here, it is formulated as a monetary loss function. If the attacker increases the amount of offensive investment, he or she could obtain a much higher but marginally diminishing value.

We call the function of what attackers obtain as the P-function, where P stands for penetration or plunder or profit. The P-function is assumed to depend on the amount of offensive investment y and the monetary loss λ of the targeted firm.

We skip discussions on how to formulate and measure offensive strength or offensive ability in the real world, which is truly a difficult question in both economics and econometrics.

On the behavior of rational attackers we could consider several things. Rational

attackers generally tend to choose targets at vulnerable firms compared with the expected value of the information of the firms. We also conjecture that the amount of offensive investment by rational attackers could not be more than the expected value of the information of the firm that they are trying to obtain. It might be possible for a short time, but not for a long time for an inefficient investment to exit. Therefore, a firm with valuable and expensive information is required to execute a larger amount of information security investment. If the information security investment is smaller, the firm system becomes more vulnerable.

The following restrictions will be assumed regarding the P-function:

A4. $\forall y$, $P(y, 0) = 0$, i.e., if the attack is not successful and its profit is 0, it stays so after every possible investment.

A5. $\forall \lambda$, $P(0, \lambda) = \lambda$, i.e., if the attacker spends no money for the investment, there will be no change in the attacker's profit.

A6. The function $P(y, \lambda)$ is continuously twice differentiable for $0 < \lambda$: $P_y = \partial P(y, \lambda)/\partial y > 0$ and $P_{yy} = \partial^2 P(y, \lambda)/\partial y^2 < 0$. Additionally, $\forall \lambda$, $\lim_{y\to\infty} P_y(y, \lambda) = 1$.

Condition A6 asserts that, with increasing investments, it is possible to increase monetary gain level, but at a decreasing rate. Nevertheless, simply by investing more amounts it is not possible to make a cyber attack arbitrarily profitable.

We will consider an example of a functional family [7] that satisfies conditions A4-A6:

$$P(y, \lambda) = 1 - (1 - \lambda)^{\theta y + 1}, \qquad \theta \succ 0. \tag{2}$$

3-2 Static Equilibrium

(1) Defender's Problem in Static Equilibrium

The expected benefit from the defensive investment, which is the reduction in the expected loss attributable to the investment, can then be computed as $(v\lambda - S(z, v)P(y, \lambda))T$, where $(v\lambda - S(z, v)P(y, \lambda))$ is the reduction in the vulnerability of the information. Part of the **remaining vulnerability** $S(z, v)$ of the information system is lost due to a cyber attack via the P-function $P(y, \lambda)$. The expected net benefit can therefore be computed as,

$$G = (v\lambda - S(z, v)P(y, \lambda))T - z. \tag{3}$$

If we do not take the attacker's point of view into account, this expression becomes $(v\lambda - S(z, v)\lambda)T - z$, the same as that formally proposed in Gordon and Loeb (2002).

Under suitable differentiability assumptions (see conditions A1-A3 above), we can see that the optimal level of the investment can be found by computing the local optimum z^* of the expected net benefit, i.e., by solving the first-order equation,

$$\partial G/\partial z = \partial\,[(v\lambda - S(z, v)P(y, \lambda))T - z]/\partial z = 0$$

and obtaining the following condition for $z^*= z^*(v, \lambda; y)$:

$$- \{\partial S(z^*, v) /\partial z\} P(y, \lambda)T =- S_z(z^*, v)P(y, \lambda)T = 1. \quad (4)$$

This shows the individual equilibrium for defenders. Let us note that a defender's decision on optimal investment is dependent on an attacker's decision.

(2) Attacker's Problem in Introductory General Dynamic Setting

An attacker extracts the total expected gain (loss of a targeted firm) $v\lambda T_t$ from a nondefending firm at a time t. However, if a defender invests z dollars in information security at τ_D, the remaining vulnerability will become the quantity denoted by $S(z, v)$. Part of the **remaining vulnerability** of the information system is lost. Then the total expected gain for the attacker will be $S(z, v)\lambda T_t$.

On the other hand, if a rational attacker invests y dollars in the system of offensive activity at τ_A, the monetary gain through the penetration denoted by the P-function towards the defending firm will increase up to $P(y, \lambda)$ from λ. Then the total expected gain obtained by the attacker will be $S(z, v)P(y, \lambda)T_t$.

Although τ_D is assumed to occur sooner than τ_A in the above discussion, a question might arise: Which is the first, τ_D or τ_A? We will later come back to this problem.

(3) Attacker's Problem in Static Equilibrium

In static equilibrium an attacker's problem is different from that in the previous introductory subsection on dynamic setting. At the time when the defender invests z dollars in information security, a rational attacker invests y dollars in the system of offensive activity at the same time. The vulnerability reduction of the defender ($v\lambda - S(z, v)P(y, \lambda)$) is assumed to go to the attacker. The attacker is assumed to try to maximize,

$$H=(S(z, v)P(y, \lambda) - v\lambda)T - y, \quad (5)$$

by determining y. This functional form of equation (5) is symmetric to that of equation (3) only in the sense that they have a zero sum only in terms of monetary gain or loss.

Under suitable differentiability assumptions (see conditions A4 - A6 above), we can see that the optimal amount of investment can be found by computing the local optimum y^* of the expected net profit, i.e., by solving the first order equation,

$$\partial H/\partial y =\partial[(S(z, v)P(y, \lambda) - v\lambda)T - y]/\partial y = 0$$

and obtaining the following condition for $y^*= y^*(v, \lambda; \mathbf{z})$:

$$S(z, v) \{\partial P(y^*, \lambda)) /\partial y\} T = S(z, v) P_y(y^*, \lambda)T = 1. \quad (6)$$

This shows the individual equilibrium for attacker. Also, note that the attacker's decision on the optimal investment is dependent on the defender's decision.

(4) Static Equilibrium

The equilibria of all individuals are dependent on each other because vulnerability other than monetary loss, i.e., the cash flow in corporation, is altered by the decisions

of others. Although this causes difficulty in the optimization calculation of a dynamic setting, in a static setting we could get rid of this difficulty.

Generally in the literature on economic equilibrium and stability in a static context, we assume that the decisions of others are instantaneously known to each other, which is called the no-time-to-learn effect. It is then definite that cyber attack suddenly appears and the damage to the defender depends on how much the information security investment is invested in.

Equations (4) and (6) are rewritten as:

$$z^* = z^*(v, \lambda; \boldsymbol{y}): -S_z(z^*, v)P(y, \lambda))T = 1, \quad (7a)$$

$$y^* = y^*(v, \lambda; \boldsymbol{z}): S(z, v)P_y(y^*, \lambda)T = 1. \quad (7b)$$

Then an equilibrium is attained if $(y^*, z^*) = (y^*(v, \lambda; \boldsymbol{z}^*), z^*(v, \lambda; \boldsymbol{y}^*))$.

The system gives us an idea on how two parties will react to each other. However, the no-time-to-learn effect is unrealistic because, in reality, it takes about several days or more for information on the installation of security tools to be obtained. Determining the nature of the static equilibrium is a starting point for analyzing the dynamics below.

(5) Stability

Is the static equilibrium stable? We can proceed formally as analyzed by Hicks (1946). Totally differentiating the above first-order conditions, we obtain

$$S_{zz}(z^*, v)P(y^*, \lambda))T\,dz + S_z(z^*, v)P_y(y^*, \lambda))T\,dy = 0, \quad (8a)$$

$$S_z(z^*, v)P_y(y^*, \lambda))T\,dz + S(z^*, v)P_{yy}(y^*, \lambda))T\,dy = 0. \quad (8b)$$

We then obtain

$$dz/dy|_F = -S_zP_y / S_{zz}P > 0, \quad (9a)$$

$$dz/dy|_L = -SP_{yy} / S_zP_y < 0. \quad (9b)$$

In these equations the symbol $|\cdot$ shows that equations (3) or (5) of $(\cdot)$ holds at maximum.

If

$$|SP_{yy} / S_zP_y| > |S_zP_y / S_{zz}P| \quad (10)$$

holds, the equilibrium is locally stable. In this equation the symbol $|\cdot|$ shows the absolute value of $(\cdot)$.

For the equilibrium to exit and be stable, various products of Equation (10) should have good properties. The stability condition (10) is satisfied under the assumptions of the functions S and P in Sections 3-1(1) and (2). Thus, the equilibrium (y^*, z^*) is locally stable. We now know that, even if some disturbing event occurs, a new equilibrium is attained immediately since both the defender and the attacker changes their optimal amount of investment.

4 Dynamics and Value Functions

To give a suitable dynamics both by a defending firm with an optimal starting time for information security investment and by an offending attacker, we extend the model of Tatsumi and Goto (2010).

First, underlying presumptions are explored. We let the trigger of a security event, T_t, follow the geometric Brownian motion with drift:

$$dT_t = \mu T_t\, dt + \sigma T_t\, dw, \tag{11}$$

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 trigger $T_0 = T$ (**unsubscripted capital letter**).

Tatsumi and Goto (2010) consider T_t as the threat of attempted breach, following Gordon and Loeb (2002). Gordon and Loeb (2002) consider 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. Here, we let T_t be the trigger. There might be expected or unexpected information arrival such as corporate announcement or news like technology invention and scheduled or unscheduled macroeconomic indicator releases. These might be a threat for defenders and a chance for attackers. The trigger evolves every moment.

Attackers could not affect the level of the trigger T_t. Their amount of offensive investment (y in our term) might affect the level of threat only through their offensive activity ($P(y, \lambda)T_t$ in our term).

The drift parameter μ in (11) could be negative although the volatility σ of the process has to be positive. Assuming the risk free interest rate r, we further assume, that

$$(r - \mu) > 0, \tag{12}$$

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

4-1 Dynamic Settings

In a dynamic setting with the addition of an attacker's perspective, the situation is quite different from that in the static setting in the previous section. Because there are two parties, a problem arises as to who invests faster, the attacker or the defender? We let the attacker's investment time be τ_A, and the defender's investment time τ_D. The times could be different.

Even if an attacker does not execute an offensive investment before a defender is protected with security tools, the defender suffers a monetary loss λ. While the defender is unprotected, however, he or she suffers much if the attacker executes the

offensive investment at τ_A. The monetary gain for the attacker (loss for the defender) will then increase from λ to $P(y, \lambda)$.

Even if the attacker executes an offensive investment by y dollars after the defender is protected with security tools at τ_D, the defender suffers monetary loss. The vulnerability reduction of the defender ($v\lambda - S(z, v)P(y, \lambda)$) becomes the monetary gain of the attacker.

4-1-1 Preemptive Attack

We suppose that an attacker invests first at $\tau_A = 0$, earlier than a targeted defender ($\tau_A < \tau_D$). This is like the well-known zero-day attack. The profit the attacker could obtain depends on how the targeted firm behaves or has behaved. Thus, we have to formulate the behavior of the defender first in order to know the profit of the attacker.

The defender maximizes the present expected benefit from the security investment for its entire life by choosing the investment time τ_D:

$$F_D(T) = \sup_{\tau_D \in \mathrm{T}} E\left[\int_0^{\tau_D} e^{-rt} v(\lambda - P(y,\lambda))T_t dt + \int_{\tau_D}^{\infty} e^{-rt}\left\{(v\lambda - S(z,v)P(y,\lambda))T_t - z\right\}dt\right] \tag{13}$$

F comes from the first letter of "follower", while L, to appear later, comes from the first letter of "leader". There is no way a defensive firm could defend itself against a preemptive attack. This is simply because it is unprotected. The first term of (13) describes the concept in which the monetary loss changes from simply λ to $(\lambda - P(y, \lambda))$. The second term after the installment of security tools at the time τ_D could be described in the same way as in the preceding section of static behavior except for the time discounting.

The derivation of optimization could be performed similarly to that in Pindyck (1991) but more closely to that in Tatsumi and Goto (2010). Thus, we obtain the following solution:

$$\begin{aligned} F_D(T) &= E\left[\int_0^{\infty} e^{-rt} v(\lambda - P(y,\lambda))T_t dt\right] + \sup_{\tau_D \in \mathrm{T}} E\left[\int_{\tau_D}^{\infty} e^{-rt}\left\{(v - S(z,v))P(y,\lambda)T_t - z\right\}dt\right] \\ &= \begin{cases} \dfrac{v(\lambda - P(y,\lambda))T}{r-\mu} + \left(\dfrac{(v - S(z,v))P(y,\lambda)T_D}{r-\mu} - \dfrac{z}{r}\right)\left(\dfrac{T}{T_D}\right)^{\beta_1} & \text{for } T \prec T_D \qquad (14a) \\ \dfrac{(v\lambda - S(z,v))P(y,\lambda)T}{r-\mu} - \dfrac{z}{r} & \text{for } T \succeq T_D, \qquad (14b) \end{cases} \end{aligned}$$

where β_1 is the root of the characteristic equation:

$$\frac{1}{2}\sigma^2\beta^2 + \left(\mu - \frac{1}{2}\sigma^2\right)\beta - r = 0\,, \tag{15}$$

and its meaningful exact solution is

$$\beta_1 = \frac{-(\mu - 1/2\,\sigma^2) + \sqrt{(\mu - 1/2\,\sigma^2)^2 + 2r\sigma^2}}{\sigma^2} > 1.$$

The expression turns out to be greater than 1. T_D is a critical level of threat for the defender to start information security investment.

We have to assume three regularity conditions for the above optimization to have significance. Because it is formally the same as that in Tatsumi and Goto (2010), a brief explanation might be sufficient. The so called "no-bubble condition" prevents the divergence of the value function when $T = 0$. That is, it is necessary to have no value without potential threats. The "value-matching condition" states that equations (14*a*) and (14*b*) become equal at T_D. The "smooth-pasting condition" requires that the tangencies of both equations are equal.

All these three conditions determine the parameters of the above characteristic equation (15) and T_D:

$$T_D = \frac{\beta_1}{\beta_1 - 1} \frac{r - \mu}{(v - S(z,v))P(y,\lambda)} \frac{z}{r} \qquad (16).$$

We skip the derivation of (16) and other equations because it is formally the same as that in Tatsumi and Goto (2010).

Now we can go back to the attacker's problem. The attacker's expected present value depends on the defender's strategy T_D thus derived:

$$\begin{aligned} L_A(T) &= E\left[\int_0^{\tau_D} e^{-rt}\{v(P(y,\lambda)-\lambda)T_t - y\}dt + \int_{\tau_D}^{\infty} e^{-rt}\{(S(z,v)P(y,\lambda) - v\lambda)T_t - y\}dt\right] \\ &= E\left[\int_0^{\infty} e^{-rt}\{v(P(y,\lambda)-\lambda)T_t - y\}dt\right] + E\left[\int_{\tau_D}^{\infty} e^{-rt}(S(z,v)-v)P(y,\lambda)T_t dt\right] \\ &= \begin{cases} \dfrac{v(P(y,\lambda)-\lambda)T}{r-\mu} - \dfrac{y}{r} + \dfrac{(S(z,v)-v)P(y,\lambda)T_D}{r-\mu}\left(\dfrac{T}{T_D}\right)^{\beta_1} & \text{for } T \prec T_D \qquad (17a) \\ \dfrac{(S(z,v)P(y,\lambda)-v\lambda)T}{r-\mu} - \dfrac{y}{r} & \text{for } T \geq T_D. \qquad (17b) \end{cases} \end{aligned}$$

The first term in the first equation describes the value before the defender takes action at τ_D, while the second describes that about after the defender installs security tools. Optimal preemption which maximizes (17*a*) is attained at T_A^*:

$$T_A^* = \frac{\beta_1}{\beta_1 - 1} \frac{r - \mu}{v(P(y,\lambda) - \lambda)} \frac{y}{r}, \qquad (18)$$

the derivation of which is similar to that of (16).

4-1-2 Preemptive Defense

We next suppose that the defender makes a preemptive defense against the attacker and invests first at $\tau_D = 0$ ($< \tau_A$). Without the loss of generality we could let τ_D

= 0. We have to consider the behavior of the attacker first for such a purpose. As in the previous subsection **4-1-1**, we can obtain the following attacker's value:

$$F_A(T) = \sup_{\tau_A \in \mathrm{T}} E\left[\int_0^{\tau_A} e^{-rt}(S(z,v)-v)\lambda T_t dt + \int_{\tau_A}^{\infty} e^{-rt}\{(S(z,v)P(y,\lambda)-v\lambda)T_t - y\}dt\right]$$

$$= E\left[\int_0^{\infty} e^{-rt}(S(z,v)-v)\lambda T_t dt\right] + \sup_{\tau_A \varepsilon \mathrm{T}} E\left[\int_{\tau_A}^{\infty} e^{-rt}\{S(z,v)(P(y,\lambda)-\lambda)T_t - y\}dt\right]$$

$$= \begin{cases} \dfrac{(S(z,v)-v)\lambda T}{r-\mu} + \left(\dfrac{S(z,v)(P(y,\lambda)-\lambda)T_A}{r-\mu} - \dfrac{y}{r}\right)\left(\dfrac{T}{T_A}\right)^{\beta_1} & for\ T \prec T_A \qquad (19a) \\ \dfrac{(S(z,v)P(y,\lambda))T}{r-\mu} - \dfrac{y}{r} & for\ T \geq T_A. \qquad (19b) \end{cases}$$

The first term of the first equation describes the expected present value before the attacker takes action at τ_A, while the second describes that after the attacker installs offensive tools. All the regularity conditions similar to those in the above subsection define the parameters of the characteristic equation and T_A :

$$T_A = \frac{\beta_1}{\beta_1 - 1}\frac{r-\mu}{S(z,v)(P(y,\lambda)-\lambda)}\frac{y}{r} \qquad (20)$$

Now we can go to the defender's problem. The defender's expected present value depends on the attacker's strategy T_A thus derived:

$$L_D(T) = E\left[\int_0^{\tau_A} e^{-rt}\{(v - S(z,v)\lambda T_t - z\}dt + \int_{\tau_A}^{\infty} e^{-rt}\{(v\lambda - S(z,v)P(y,\lambda))T_t - z\}dt\right]$$

$$= E\left[\int_0^{\infty} e^{-rt}\{(v - S(z,v))\lambda T_t - z\}dt\right] + E\left[\int_{\tau_A}^{\infty} e^{-rt} S(z,v)(\lambda - P(y,\lambda))T_t dt\right]$$

$$= \begin{cases} \dfrac{(v-S(z,v))\lambda T}{r-\mu} - \dfrac{z}{r} + \dfrac{S(z,v)(\lambda - P(y,\lambda))T_A}{r-\mu}\left(\dfrac{T}{T_A}\right)^{\beta_1} & for\ T \prec T_A \qquad (21a) \\ \dfrac{(v\lambda - S(z,v)P(y,\lambda))T}{r-\mu} - \dfrac{z}{r} & for\ T \geq T_A. \qquad (21b) \end{cases}$$

The optimal preemption that maximizes (21a) is attained at T_D^*:

$$T_D^* = \frac{\beta_1}{\beta_1 - 1}\frac{r-\mu}{(v - S(z,v))}\frac{z}{r}, \qquad (22)$$

the derivation of which is similar to that of (16).

4-2 Who is the preemptor?

We have to raise a fundamental question and restate our problem. The question is who the preemptor is going to be.

(1) General Framework ~ Aggressive Attack and Active Defense

There is a well-known principle of the leader-follower relationship that states that when the value for an entity needed to become the leader is larger than that needed

to become the follower, the entity becomes the leader.

The leader could choose whether he or she becomes the preemptor or not, while the follower has to accept how the leader behaves. One could be the preemptor even if one is not the leader. If the attacker who becomes the leader chooses not to attack, the defender might become an unintended preemptor. Therefore, both an intended preemptor and an unintended preemptor exist for both sides of the battle.

If the attacker becomes the leader and preemptor, it might be an aggressive attack. If the defender becomes the leader and preemptor, on the other hand, it might be an intended defense. Alternatively, it is called the "active defense", which might be what security vendors have called it recently.

(2) Conditions of Leadership and Preemption ~ How the Leader Behaves

The attacker or defender has the incentive to become the leader, depending on whether his or her present values are larger when he or she becomes the leader. Therefore, they might be critically the leader and possibly the preemptor at $\overline{T}_A$ or $\overline{T}_D$ which satisfies the equation

$$L_I(\overline{T}_I) = F_I(\overline{T}_I), \qquad I = A, D. \tag{23}$$

Who starts first to behave is determined by which is smaller (shorter), $\overline{T}_A$ or $\overline{T}_D$. The leader is defined as the entity that makes the earlier or quicker (shorter) decision.

We will describe how the leader decides the timing of preemption later in this subsection. Optimization is meaningfully attained only when one is the leader, as stated in the above subsection. Therefore, it will be naturally considered that $\overline{T}_I$ is smaller (that is, shorter) than T_I^*.

If one becomes the leader, one could also be the preemptor. If $\overline{T}_D < \overline{T}_A$, the defender is the leader and possible preemptor, while the attacker is the leader and possible preemptor if $\overline{T}_D > \overline{T}_A$.

More accurately stated, there are four possibilities under the preceding optimal preemption conditions:

(i) If $T_D^* < \overline{T}_A$, the defender's intended and optimal preemption occurs at T_D^*.

(ii) If $\overline{T}_D < \overline{T}_A < T_D^*$, the defender's intended preemption occurs at $\overline{T}_D$.

(iii) If $T_A^* < \overline{T}_D$, the attacker's intended and optimal preemption occurs at T_A^*.

(iv) If $\overline{T}_A < \overline{T}_D < T_A^*$, the attacker's intended preemption occurs at $\overline{T}_A$.

The condition $T_D^* < \overline{T}_A$ (or $T_A^* < \overline{T}_D$) implies that $\overline{T}_D < T_D^* < \overline{T}_A < T_A^*$ (or $\overline{T}_A < T_A^* < \overline{T}_D < T_D^*$), therefore, it shows that the defender (or attacker) becomes the leader and preemptor. This describes possibility (i) or (iii).

Generally, whether $\overline{T}_I$ is smaller (shorter) than T_I^* determines whether leader

I could perform an optimal start. If $\overline{T}_I$ is smaller (shorter) than $\overline{T}_J$ and $\overline{T}_J$ is also smaller (shorter) than T_I^* (so that $\overline{T}_I < \overline{T}_J < T_I^*$), however, the leader *I* could wait for the preemptive attack until T_I^*, with a possibility of losing the preemptive position. Hence, the leader *I* executes the preemptive attack at $\overline{T}_I$ before T_I^*. This is the reason why the leader chooses a preemptive strategy that is not optimal. These argument describes possibility (ii) or (iv).

This completes the combination of $\overline{T}_I$ and T_I^* for $I = A, D,$ because $\overline{T}_I$ is considered to be smaller (shorter) than T_I^*.

4-3 Optimal Solutions of Investment

Optimal solutions consist of both the investment time and the amount of investment. Firstly, the timing of preemption has been given so far.

Next, we find the optimal amount of the follower's investment, which is attained by maximizing the expected benefit from the investment at T_i:

$$y_A = \arg\max_{y \varepsilon R} F_A(T_A; y), \tag{24}$$

$$z_D = \arg\max_{z \varepsilon R} F_D(T_D; z). \tag{25}$$

Furthermore, the optimal amount of the preemptor's investment is given by

$$y_A^* = \arg\max_{y \varepsilon R} L_A(T_A^*; y), \tag{26}$$

$$z_D^* = \arg\max_{z \varepsilon R} L_D(T_D^*; z). \tag{27}$$

Note that y_A^* depends on y_A and z_D through T_D and T_A^*, respectively. Similarly, y_D^* depends on z_A and y_D through T_A and T_D^*, respectively. That is, the amounts of the attacker's and defender's investments depend on each other, not only on timing.

Finally, we determine who will be the preemptor by comparing T_A^* with T_D^* after the maximization by the amount of investment.

The concrete expressions for y_A and z_D are

$$y_A = \frac{\ln \dfrac{r-\mu}{r} - \ln\left(-\theta S(1-\lambda)T_A \ln(1-\lambda)\right)}{\theta \ln(1-\lambda)}, \tag{28}$$

$$z_D = \frac{\ln \dfrac{r-\mu}{r} - \ln\left(-\alpha v P T_D \ln v\right)}{\alpha \ln v}, \tag{29}$$

respectively. Those for y_D^* and z_D^* [8] are similar except that T_A and T_D are replaced

with T_A^* and T_D^*, respectively.

4-4 Nature of the Model Restated

(1) Asymmetric Nature of Model and Market Failure

Akerlof (1970) is the first to analyze the quality of goods and raised the well-known notion of an information asymmetry between supply and demand, using the example of used cars (lemons). He then described the resulting market structure (sometimes called the winner's curse) that higher-quality goods disappear from the market.

Preceding research studies or prior WEIS workshops have explored the role of incentives between attackers and defenders of information systems, and identified market failures surrounding Internet security.

The situation to be considered in the context is clearly different from either Gordon et al. (2003) or agency (cost) problems between borrowing firms and lending banks elaborated in many research studies since the work of Jensen and Meckling (1976).

One may ask, "Is the phenomenon that has been described and is discussed in the following sections one of the market failures?" If an individual disturbs others' activities, or destroys a safe order when the others are doing an activity, and if he or she is not forced to pay for the use of such resources as public order or economic order, then this cost will be borne not by the individual (cyber attacker) but by others or the society.

Conventional markets are institutions that organize the exchange of control of commodities or services, where the nature of the control is defined by the property rights attached to the commodities or services.

The underlying market that we are discussing is that of keeping a safe public or economic order. Cyber threat compulsorily supplied by attackers is a bad in economics. It constitutes a market where bads are supplied too much from the viewpoint of defenders. However, the market mechanism could not solve the oversupply problem.

Hence, the market price for keeping a safe order will fail to incorporate the full opportunity cost to the society of producing it. In the case under consideration, the market equilibrium in the orderly circumstance will not be optimal. More disorder will be produced than would occur were the individual to pay for all the costs of producing the orderly circumstance [9].

(2) Zero-Sum Game

In the game theory or economic theory, a zero-sum game is a mathematical representation of a situation in which a participant's gain (or loss) of utility is exactly balanced by the losses (or gains) of the utility of other participants. If the total gains of

the participants are added up, and the total losses are subtracted, they will sum to zero. A zero-sum game is also called a strictly competitive game. Zero-sum games are most often solved with the Nash equilibrium.

In contrast, a non-zero-sum game describes a situation in which the interacting parties' aggregate gains and losses are either less than or more than zero.

We have postulated that an information security game is not a non-zero-sum game and that in such a game an attacker' gain is from its defender's value.

(3) Timing Problem and Sunk Costs

It might take a longer time than expected for attackers to obtain the fruit of their effort. This is especially so in order to establish the attacker's own competitive status when confidential information is stolen or a crucial function of a targeted firm is shut down. The analysis of cyber attack should therefore be taken from a longer point of view. For this purpose, a real options theory approach is suitable.

Costs incurred by a preemptive defense or attack might become sunk cost. "When market conditions evolve unpredictably (as they often do), firms incur an opportunity cost when they invest in new capital because they give up the option to wait for the arrival of new information about the likely returns from the investment. This option value is a sunk cost [Pindyck (2008)]."

(4) Preemptive Defense

There is a proverb saying that attack is the best form of defense. This is about a strategy of defenders towards attackers and now is the conventional wisdom for preemptive strikes. The words by Washington are also often referred to that offensive operation is the surest, if not the only, means of defense.

However, cyber defense is quite different from any previous actual war. Since defenders could neither see attackers coming nor know when they come, the preemptive strike for the defender side in cyber security is almost limited to preemptive defense.

Furthermore the proverb does not take account of both the monetary gain (loss) and the offensive technology. If the monetary loss caused by sacking is small, no defender will take any action. On the other hand, attackers become especially active if the monetary gain is large.

On the offensive technology, the attackers could not do anything special without it. However, the defender does not necessarily know its efficiency.

5 Numerical Illustrations

5-1 Procedure of Numerical Calculation

(1) Assumptions of Numerical Calculation

Numerical illustrations, the only way we could know the detailed properties of the solution, are needed because functional relationships among variables are implicit. In this section, we numerically calculate the optimal investment threshold *Ts* and the optimal amount of investment *y* or *z* to determine the properties of the model solution built.

Although the preceding research studies up to Gordon and Loeb (2002) took two numerical examples, we only consider only one case, i.e., Case II. This is because *z** turns out to be insensitive to the change in *v* in Case I. To perform the calculation, therefore, we use Case II: $S^{II}= v^{\alpha z+1}$, ($\alpha > 0$) for the remaining vulnerability *S* function.

We will present a comparative statics analysis of the threshold *Ts* and amount of investment *y* or *z* with a change in the following parameters: volatility σ, efficiency of attack θ, vulnerability *v*, monetary value λ (gain or loss), and the parameter of remaining vulnerability function α.

Since the volatility σ represents the degree of uncertainty, it is the most important parameter among the above parameters in a real options model. We will study this in the case of the zero-sum information security game. The monetary value λ (gain or loss) and the efficiency of attack θ are quite new variables on which we will concentrate our focus.

(2) Calculation Procedure

In Tatsumi and Goto (2010), the fixed-point problem, $z^* = z\ (T^*(z))$ was calculated by an iterative procedure. On the other hand, the calculation procedure of our zero-sum game model proceeds from a fixed-point problem: $y_A(T_A) = y_A^*(T_A^*)$ and $z_D(T_D) = z_D^*(T_D^*)$, optimal response: $y_A^*(z) = y_A^*(y_A^*, z_D^*)$ and $z_D^*(y) = z_D^*(y_A^*, z_D^*)$, and equilibrium: (y_A^*, z_D^*).

The fixed-point problem describes that the optimal investment is attained at T_A^* or T_D^*. An optimal response function is needed because the optimization processes by both the attacker and the defender become mutually dependent. The interaction results in an equilibrium.

An infinite loop may occur because both the optimization processes are mutually dependent. This creates a difficulty. We avoid this difficulty in the loop by limiting optimization, i.e., by abandoning nuisance cases of nonoptimal preemption.

The calculation procedure of the model in the current setting now becomes as follows:

1. Fixed point problem: $y_A(T_A) = y_A^*(T_A^*)$ and $z_D(T_D) = z_D^*(T_D^*)$,
2. Optimal response: $y_A^*(z) = y_A^*$ and $z_D^*(y) = z_D^*$,
3. Equilibrium: (y_A^*, z_D^*).

Procedure 1 describes the optimal investment. The optimal response function is linear, independently of others' behavior.

5-2 Results of Numerical Calculation

We assume that the hypothetical base values of the parameters are as follows: σ = 0.2, $\mu = 0.02$, $r = 0.05$, $v = 0.5$, $\lambda = 0.5$, $\alpha = 1$ and $\theta = 1$ as shown in **Table 1**.

The parameter values in the bottom six lines of **Table 1**, needed because the optimization processes by both the attacker and the defender become mutually dependent, are derived after a tentative calculation is attempted several times.

Table 1. Base Case Parameter:

σ	Volatility	0.2
μ	expected growth rate	0.02
r	discount rate	0.05
v	Vulnerability	0.5
λ	monetary loss	0.5
α	S-function	1
θ	P-function	1
z_D^*	defender's optimal investment	2.53
y_A^*	attacker's optimal investment	2.53
$S(z_D^*, v)$	remaining vulnerability	0.087
$P(y_A^*, \lambda)$	increased monetary loss	0.91
$T_D^*(z_D^*)$	defender's threshold	19.96
$T_A(y_A^*)$	attacker's threshold	115.02

The effect of a specific parameter, while others are fixed at the value in **Table 1**, is calculated in the following subsections. The shortest Ts are highlighted in bold, which shows preemption. In the following **Tables**, the bar – means that $\overline{T}_A$ does not exist in each case.

(1) Effects of Vulnerability and Monetary Value

Table 2 examines the effects of the vulnerability v and the monetary value λ (gain or loss) on the preemptive decision and the amount of investment.

If a target firm is extremely highly vulnerable (higher v), an attacker executes a leadoff attack. This could be performed even with a relatively smaller amount of investment y_A^*. On the other hand, a defending firm with a low vulnerability will defend itself preemptively, but it is so only in the case of smaller amount of investment z_D^*.

Table 2. Comparative Statics: v and λ

v	z_D^*	T_D^*	$\overline{T}_D$	y_A^*	T_A^*	$\overline{T}_A$
0.1	0.76	**30.05**	9.75	2.53	99.85	-
0.3	1.45	**19.16**	6.30	2.53	33.29	-
0.5	2.53	**19.96**	6.65	2.53	19.96	-
0.7	4.91	27.71	9.50	2.53	14.26	**5.30**
0.9	16.63	72.99	28.40	2.53	**11.10**	2.50
λ	z_D^*	T_D^*	$\overline{T}_D$	y_A^*	T_A^*	$\overline{T}_A$
0.1	2.53	**99.85**	5.75	16.63	72.99	-
0.3	2.53	**33.29**	6.20	4.91	27.71	-
0.5	2.53	**19.96**	6.65	2.53	19.96	-
0.7	2.53	**14.26**	7.20	1.45	19.16	-
0.9	2.53	11.10	8.10	0.76	30.05	**1.65**

In fact if v is 0.9, the attack is very quickly performed in the boldfaced time of 11.10 time units. The offensive investment could be made even with a relatively smaller amount of 2.53 in the numerical example of the investment y_A^*. If v is 0.3, on the other hand, the attack is not preemptively performed. Furthermore this requires the same amount (2.53 in the numerical example) of investment y_A^*. Regarding the defensive side, if v is 0.3, the security investment is made in the boldfaced relatively quicker at 19.16 time units. This could be made even with a relatively smaller amount (1.45 in the numerical example) of investment z_D^*.

The attacker would not, however, invest a larger amount to attack a target with a low vulnerability. Therefore, a defender with a low vulnerability inevitably becomes the preemptor (unintended and **unnecessary** preemption).

Thus it seems that the attacker is more rational than the defender since the defender defends itself because the cost is lower, while the attacker behaves depending on the vulnerability. It is interesting to know that the asymmetry between the behavior of the attacker and that of the defender arises from the simple behavioral model described above.

Regarding the monetary value (gain), we observe a very similar pattern. If the monetary value (gain) is larger, the attacker will be the preemptor. Furthermore, the required amount of investment is minimal. In other cases of intermediate and smaller monetary values (losses), the defender will be the preemptor.

If λ is 0.9, the attack is very quickly performed in the boldfaced quickest time of 1.65 time units. This could be performed even with relatively smaller amount (the smallest 0.76 in the numerical example) of the investment y_A^*.

As for the relationship between y_A^* and λ, the result of investment efficiency is also as expected above. If y_A^* is larger than λ, no preemptive attack is observed. This is another nature of the rational attacker. Attacker never invests in attacking a target with little returns. We see in fact from **Table 2** that the attacker becomes the preemptor only when the monetary gain λ is 0.9 and the amount of investment is 0.76. While λ is between 0.1 and 0.7, $\overline{T}_A$ does not exist.

Overall it could be summarized from **Table 2** that preemptive attack occurs, as expected, at a high vulnerability and a large monetary gain. Thus, rational attackers are very rational.

It is optimal, as a warning to be concluded from the analysis, that vulnerable defenders should become the preemptor even with a large amount of investment. However, the defender in the model behaves differently.

(2) Effects of Efficiency of Attack and Volatility

The effects of the efficiency of attack θ and the volatility σ on preemptive decision and the amount of investment are shown in **Table 3**.

Table 3. Comparative Statics: θ and σ

θ	z_D^*	T_D^*	$\overline{T}_D$	y_A^*	T_A^*	$\overline{T}_A$
1	2.53	**19.96**	6.65	2.53	19.96	-
2	2.53	19.96	6.85	1.27	9.99	**3.60**
3	2.53	19.96	7.05	0.84	**6.65**	1.80
4	2.53	19.96	7.20	0.63	**5.00**	1.25
5	2.53	19.96	7.40	0.51	**4.00**	0.95
σ	z_D^*	T_D^*	$\overline{T}_D$	y_A^*	T_A^*	$\overline{T}_A$
0.1	1.81	**12.16**	4.10	1.81	12.16	-
0.2	2.53	**19.96**	6.65	2.53	19.96	-
0.3	3.21	**32.15**	10.90	3.21	32.15	-
0.4	3.84	**49.51**	17.20	3.84	49.51	-
0.5	4.40	**72.88**	26.10	4.40	72.88	-

Preemptive attack occurs at a high efficiency of attack. At a lower efficiency of attack, however, attackers give up (evade) any preemptive strike simply because it has to be with inefficient technology and requires a larger amount of investment (as seen from **Table 3**, the amount of investment is highest at 2.53 when θ=1). Then an

unintended preemptive defense occurs.

The volatility σ does not affect the decision of the attacker whether he or she is willing to be the preemptor. Contrary to the fact that volatility is usually the most important parameter in a real options model, its importance is different for the current zero-sum game cyber-battle model. This constitutes another nature of the current model.

(3) Effects of Efficiency of Attack

Table 4 shows the effects of the efficiency of attack θ on the preemptive decision and the amount of the investment when $v = 0.1$ and $\lambda = 0.1$.

Table 4.Comparative Statics: θ with $v = 0.1$ and $\lambda = 0.1$

$v = 0.1$

Θ	z_D^*	T_D^*	$\overline{T}_D$	y_A^*	T_A^*	$\overline{T}_A$
1	0.76	**30.05**	9.75	2.53	99.85	-
3	0.76	**30.05**	10.00	0.84	33.29	-
5	0.76	**30.05**	10.20	0.51	19.96	-
7	0.76	30.05	10.35	0.36	14.26	**4.80**
9	0.76	30.05	10.55	0.28	11.10	**3.15**

$\lambda = 0.1$

Θ	z_D^*	T_D^*	$\overline{T}_D$	y_A^*	T_A^*	$\overline{T}_A$
1	2.53	**99.85**	5.75	16.63	72.99	-
3	2.53	**99.85**	5.90	5.55	24.34	-
5	2.53	**99.85**	6.05	3.33	14.60	-
7	2.53	**99.85**	6.20	2.38	10.43	-
9	2.53	**99.85**	6.30	1.85	8.11	-
11	2.53	99.85	**6.40**	1.51	6.64	8.65

It is partly true that the defender becomes the preemptor depending on his or her monetary loss. Even if the monetary loss is small and the efficiency of attack is low, however, the defender becomes the preemptor. This is simply because the attacker does not move.

If $\lambda = 0.1$ and θ=11, that is, there is a higher efficiency of attack even with a larger monetary gain, the attacker could not attain optimal preemption.

Table 5 shows the effect of the efficiency of attack θ on the preemptive decision and the amount of investment when σ = 0.5. If the efficiency of attack θ is high, preemptive attack occurs. An attacker never misses the chance to exploit the technical possibility. Only if the efficiency of attack θ is low, however, does preemptive defense

occur. This fact is contrary to what information security investment should be. If the level of offensive technology is higher, an attacker responds more quickly although a defending firm should execute information security investment.

Table 5. Comparative Statics: θ with σ = 0.5

Θ	z_D^*	T_D^*	$\overline{T}_D$	y_A^*	T_A^*	$\overline{T}_A$
1	4.40	**72.88**	26.10	4.40	72.88	-
2	4.40	**72.88**	26.10	2.20	36.44	-
3	4.40	72.88	27.10	1.47	**24.29**	6.80
4	4.40	72.88	27.45	1.10	**18.21**	4.15
5	4.40	72.88	27.75	0.88	**14.58**	2.95

(4) Effects of Efficiency of Security

Table 6 shows the effect of information security technology. We observe from **Table 6** that an attacker is indifferent to the level of security technology. Even when the level of security technology α is low, an attacker responds very slowly.

On the other hand a defender responds to the level of the technology as follows. As the level of security technology α increases the defender comes to respond more quickly to be the preemptor with a smaller amount of investment. Although this is what information security investment has to be, that is, the defender should not be indifferent to the level of security technology, the sensitivity is slightly wasted considering the attacker's slow response.

Table 6. Comparative Statics: α

α	z_D^*	T_D^*	$\overline{T}_D$	y_A^*	T_A^*	$\overline{T}_A$
1	2.53	**19.96**	6.65	2.53	19.96	115.00
2	1.27	**9.99**	3.25	2.53	19.96	115.30
3	0.84	**6.65**	2.15	2.53	19.96	115.00
4	0.63	**5.00**	1.60	2.53	19.96	115.30
5	0.51	**4.00**	1.25	2.53	19.96	115.30
6	0.42	**3.34**	1.05	2.53	19.96	115.85
7	0.36	**2.85**	0.90	2.53	19.96	115.00
8	0.32	**2.50**	0.80	2.53	19.96	115.30
9	0.28	**2.21**	0.70	2.53	19.96	114.15
10	0.25	**2.00**	0.60	2.53	19.96	115.30

6 Concluding Remarks

6-1 Summary

We formulated a two-player zero-sum game of both information security and offensive investments from the defender's and attacker's perspectives in terms of a real options theory and analyzed how cyber attackers behave under reasonable assumptions and highlight preemptive attack like the zero-day attack. We also analyzed when and how defenders respond towards such an attacker.

(1) Theoretical Points

We assumed that defenders focus on their vulnerability when defending, while attackers focus on the monetary gain rather than the defenders' vulnerability when they execute an attack. These formulations are represented by the function $P(y, \lambda)$ and also by $S(z, v)$.

Under this model, the conclusion that the information security investment is of use is derived. We also find that the timing of the attacker's and defender's investments depend not only on each other, but also on the amount of investment.

Furthermore, it is theoretically interesting that, although the function $P(y, \lambda)$ does not depend on vulnerability, the attacker is shown very sensitive to it.

(2) From Numerical Results

The findings of our numerical calculation reported are consistent with Verizon (2012), that investigated data breach and concludes that cybercriminals automate and streamline their method du jour of high-volume, low-risk attacks against weaker targets.

Through numerical analyses, attackers are turned out to be rational in the sense that they become very sensitive and quickly respond to both the monetary gain they will obtain and the vulnerability of defenders. If attackers could preempt, they immediately invest a small sum of money. The efficiency of attack has large impact on the decision, but the monetary gain is more important for attackers.

Defenders' intended and optimal preemption occurs and the optimal preemption condition ① never occurs in our numerical assumption. In many cases, defenders can preempt optimally. However, this is so because attackers have no incentive to attack targets with a smaller monetary gain.

6-2 Unsolved Economic Problems

(1) Free Rider Problem

Defenders might wait to utilize an opportunity until the price of a security tool goes down since many other defenders suffer and hurry to install it and eventually its price changes. The price goes down if the security tool is produced in large quantity or

if security venders develop a cheaper tool. Some defenders wait for an opportunity of the installment, therefore, until the price goes down.

Gordon et al. (2003) firstly pointed out such a problem by building a game-theoretic model of two companies with information sharing. The picture is different if we include attackers in the model. Although the problem might have complicated features, it will be an interesting future work to include an attacker or attackers into the Gordon et al. (2003) model.

(2) Sunk Cost and Functional Form of Risk Function

The usability of a model could be determined by how the model gives a solution to such different situations as follows: one security tool protecting against multiple threats, multiple threats attacking a single vulnerability and several security tools protecting against one threat. A model with multiple attackers and multiple defenders is thus what we need.

At the same time researchers are faced with two very serious problems on vulnerability: how to measure vulnerability and how to deal with various vulnerabilities.

The first problem is rather empirical, but very important and very difficult to solve. The expenditure for preemptive defense (that is, the installment of security tools before any cyber attack) may become sunk cost or may be conceived as sunk cost because its effectiveness is not understood and people think of it as simply a waste finances.

However if we can measure vulnerability accurately and everyone accepts the validity of such measurement, the problem is solved. People think then that it is not a waste of time to carry out such a thing, and the installment will prove to be of use someday.

Can we add various vulnerabilities? The answer to this is generally no. Several theoretical papers in WEIS adopt the following ordinal approach. The total vulnerability of a firm is composed of a vector: (vulnerability of the first subsystem, vulnerability of the second subsystem, vulnerability of the third subsystem, and so on). Firms are then supposed to try to maximize the expected benefit vector of total vulnerability reduction (or to minimize the total vulnerability).

The problem might become complex if we include attackers into these models.

(3) Other Future Works

How much of the *P*-function defined and analyzed above is applicable in the real world? We are not claiming that the functional form of the *P*-function considered is unquestionable. A realistic and rational setting for the *P*-function is needed, and its economic implications should be investigated further.

A natural extension of the present model might be the inclusion of the vulnerability variable v into the P-function: $P(y, v, \lambda)$ instead of $P(y, \lambda)$. Correspondingly, we have to change the remaining vulnerability function to $S(z, v, \lambda)$ instead of $S(z, v)$. Then the model becomes strictly symmetric, and it becomes very difficult to theoretically solve and numerically simulate the optimal solution.

Both technological progress and its gap might affect our conclusion. Technological progress might have positive effects on information security investment if offensive ability grows faster than defense ability and if it is known to the defender. It is also conceivable that if defensive tools are more efficient than offensive tools, defenders might have a different decision. However, as present, we have no appropriate analytical tools yet for treating the effect of differential technological progress.

FOOTNOTES

1) More trends have been observed in which attackers seem to employ more and more human and social factors in their attacks. The so-called social engineering is utilized by counting on others' or even user's help for support.

Firms invested in outside/in defense have been urged to invest in inside/out defense as well, which is in other words a trend from perimeter defense to encryption, access control and other strategies.

2) Some other general trends concerning the nature of information security technology and investment could be summarized as follows. The level of information security that has been attained using past investment could be made obsolete immediately owing to cyber attack. The new technology of information security is embodied only in new investments, so that we need surely a vintage type theory of investment. The exploration of the theory towards this direction might be a future work for us.

3) A mathematically fair game is one in which each player has just as much chance of winning as of losing and the expected value of the outcome is zero. If a fair game is played, you might end up winning or losing depending on your luck, but the average gain or loss per play calculated over all repeated plays will tend towards zero with time.

4) From Wikipedia, Canada is reportedly losing $12 billion and German companies are estimated to be losing about $87 billion and 30,000 jobs to industrial espionage every year.

5) A more realistic adaptive model for an (s, S)-type inventory investment procedure for information security is studied by Goto and Tatsumi (2012). In this model, both adjustment cost and a real options theory play important roles.

6) A market that has only one supplier and one buyer is called bilateral monopoly. The supplier will tend to act as that in a monopoly, and charge the sole buyer a higher price. The buyer will look towards paying the lowest price possible. Since both parties have conflicting goals, the two sides must negotiate on the basis of the relative bargaining power of each other, with the final price settling in between the two sides' points of maximum profit.

7) Although previous studies showed two numerical examples, we only consider the example corresponding to case II of the *S*-function. The example corresponding to case I given by,

$$P(y,\lambda) = 1 - \frac{1-\lambda}{(\theta y\lambda + 1)^{\eta}}, \qquad \theta \succ 0,\ \eta \in R$$

shows no interesting results, possibly because the optimal behavior y^* is not sensitive to the change in the vulnerability v.

8) The expressions for optimal information security investment in the other cases are, interesting for comparison, as shown below:

$$z = \frac{-\ln(-\alpha v\lambda T \ \ln v)}{\alpha \ln v}$$

for Gordon and Loeb (2002).

$$z = \frac{\ln\frac{r-\mu}{r} - \ln(-\alpha v\lambda T \ \ln v)}{\alpha \ln v}$$

for Tatsumi and Goto (2010). Thus, the expression in the text is a generalization of both cases.

9) Market failures are often associated with information asymmetries, noncompetitive markets, principal-agent problems, externalities, or public goods. The occurrence of market failures is often used as a justification for government intervention in a particular market. What we need in the case under consideration might be a cyber police to maintain order.

REFERENCES

Akerlof, G. A., (1970), "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism," *Quarterly Journal of Economics*, 84 (3), Aug. 1970, pp. 488-500.

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. A., Loeb, M. P. and Lucyshyn, W., (2003), "Sharing Information on Computer Systems Security: An Economic Analysis," *Journal of Accounting and*

Public Policy, 22, pp.461-485.

Goto, M. and Tatsumi, K., (2012), "The Theory of Optimal Investment in Information Security and Adjustment Costs: An Impulse Control Approach," pp. 73-96 in *Recent Advances in Financial Engineering 2011, Proceedings of International Workshop*, edited by Takahasi, A., Muromachi, Y. and Nakaoka, H., World Scientific Publishing, 2012.

Hicks, J. R., (1946), *Value and Capital,* 2nd ed., Oxford: Clarendon Press.

Jensen, M. C. and Meckling, W. H., (1976), "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure," *Journal of Financial Economics*, 3 (4): pp.305-360.

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

Pindyck, R. S., (2008), "Sunk Costs and Real Options in Antitrust Analysis," in *Issues in Competition Law and Policy*, ABA Press, 2008.

Willemson, J., (2006), "On the Gordon & Loeb Model for Information Security Investment," The Fifth Annual Workshop on Economics and Information Security (WEIS2006).

Tatsumi, K. and Goto, M., (2010), "Optimal Timing of Information Security Investment," The Eighth Annual Workshop on Economics and Information Security (WEIS2009). (http://weis09.infosecon.net/files/112/index.html) Also chapter 11 in Moore, T., Pym, D. and Ioannidis, C. (eds.), *Economics of Information Security and Privacy*, Springer, 2010.

Verizon (2012), *Verizon 2012 Data Breach Investigations Report.* http://www.verizon.com/enterprise/2012dbir/jp