# Economics of Information Security Investment in the Case of Simultaneous Attacks

C. Derrick Huang
Department of Information Technology & Operations Management
College of Business
Florida Atlantic University
Boca Raton, FL 33431
dhuang@fau.edu

Qing Hu
Department of Information Technology & Operations Management
College of Business
Florida Atlantic University
Boca Raton, FL 33431
qhu@fau.edu

Ravi S. Behara
Department of Information Technology & Operations Management
College of Business
Florida Atlantic University
Boca Raton, FL 33431
rbehara@fau.edu

Manuscript to be presented at
*The Fifth Workshop on the Economics of Information Security (WEIS 2006)*

# Economics of Information Security Investment in the Case of Simultaneous Attacks

## ABSTRACT

With billions of dollars being spent on information security related products and services each year, the economics of information security investment has become an important area of research, with significant implications for management practices. Drawing on recent studies that examine optimal security investment levels under various attack scenarios, we propose an economic model that considers simultaneous attacks from multiple external agents with distinct characteristics, and derive optimal investments based on the principle of benefit maximization. The relationships among the major variables, such as systems vulnerability, security breach probability, potential loss of security breach, and security investment levels, are investigated via analytical and numerical analyses subject to various boundary conditions. In particular, our model shows how a firm should allocate its limited security budget to defend against two types of security attacks (distributed and targeted) simultaneously. Among the results of these analyses, we find that a firm with a small security budget is better off allocating most or all of the investment to measures against one of the classes of attack. Further, when the potential loss from the targeted attacks and the system vulnerability are relatively large, the focal firm should allocate most of its budget to such attacks.

***Keywords: Information Security, Security Investment, Economic Modeling, Optimal Investment***

## 1. Introduction

In the era of the commoditization of information technology (IT) and the globalization of world economy, it is argued that the most challenging aspect of managing today's networked organizations is not so much using IT to create competitive advantages in the marketplace but managing the potential risks created by IT (Carr, 2003). And among the risks, security breach to the highly connected corporate information systems is perhaps the most prominent and visible, as evidenced in the headlines of mass media in recent years. In a 2003 survey of the Global 500 companies, 39% of the respondents reported that their information systems had been compromised in some way in the prior year (Power, 2003). And the general (and seemingly natural) reaction to this growing risk has been increased spending on security technologies. While worldwide IT spending has remained flat or even slightly down in recent years after the burst of Internet bubble in 2000, spending on information security related products and services by organizations large and small has been growing at a rate of 17.6% per annum and is forecasted to reach $21.6 billion in 2006 (AT&T, 2004).

However, it is commonly recognized that complete information security at the corporate level is virtually impossible without hindering the normal business activities in today's economy, where connectivity to external business partners and customers is essential. Given the unattainable state of complete security, in recent years, scholars and practitioners alike seek to address a different question about information security: How does a firm *minimize* security risks with limited resources for implementing security technologies and programs? This question has spawned two distinct yet complementary streams of research: The determination of return on security investments (ROSI) (Cavusoglu et al., 2004, 2005) and the search for optimal security investment levels under different security threat scenarios (Gordon and Loeb, 2002; Huang et al., 2005a, 2005b). In this paper, we draw on the prior works in the latter stream and examine the optimal investment levels under a more realistic set of boundary conditions and assumptions. Specifically, we develop security investment optimization models that consider simultaneous attacks on the focal information system by two types of external threats: the distributed attack, such as computer viruses and spyware lurking for opportunities through random but massive campaigns, and the targeted attack, via which hackers attempt to break into specific systems to destroy, alter, or steal valuable data and information. In so doing, we hope to advance the knowledge of economics of information security and to provide insight into better information security management practices.

The rest of the paper is arranged as follows. In the next section, we review the recent development in the area of economics of information security and identify the gaps in the research literature. In section 3, we develop the core economic model of information security investment for managing the aforementioned two types of security breaches. This model is then used to yield optimal security investments without (in section 4) and with (in section 5) the constraint of security budget. Numerical analyses are also performed to provide insights into the behaviors of the model and the interactions of the variables under different scenarios. Finally, in section 6, we discuss the main findings of this study in the context of information security practices. Limitations of the current approach and future research directions for further advancing the research stream are also discussed.

## 2. Research Background

Research in the area of the economics of information security investment, where the traditional decision analysis in determining the optimal level of investments based on risk and return, is still in its early stage. Adopting the assumption of risk neutrality, Gordon and Loeb (2002a) analyze the optimal level of security investments based on the principle of maximizing the net benefit of such investments. They find that the optimal investment in information security does not necessarily increase with vulnerability, implying that a firm should not always invest to protect the most vulnerable information systems. They also show that the optimal security investment would be far less than the potential loss (with a theoretical maximum of 36.8%) due to a security breach.

Huang et al. (2005a, 2005b) extend the above model by taking into account the risk profile of the decision maker of the firm in question and adopt the expected utility theory in optimizing the information security investment. When the decision maker is risk averse—a commonly accepted assumption for firms with good performance (Fiegenbaum and Thomas, 1988; Jegers, 1991)—they find that the optimal information security investment is zero below a minimum potential loss; above that minimum, optimal investment does increase with potential loss. And, contrary to the risk-neutral case, a risk-averse decision maker may make security investment close to (but never exceeds) the potential loss in the case of distributed attacks. In addition, they find that a decision maker more averse to risk (i.e., with less appetite in accepting risk) does not necessarily invests more in information security.

In the case of firms with interconnected IT systems, Ogut, Menon, and Raghunathan (2005) find that such interdependency reduces the firms' information security investments to a level lower than optimum. In contrast, when these interconnected firms face liability in IT security—the breached firm has to pay others for collateral damages—they tend to over-invest above the optimal level. This is because each firm can only optimize its own utility, even though some of the risks are controlled by other interconnected firms. Consequently, the investment decision reached under such constraint is almost always sub-optimal, unless all interconnected firms can plan and optimize their information security investment jointly.

So far, these economic studies have focused on optimizing the *total* investment in information security. But today's firms face different types of security challenges at the same time. The most common are the *distributed attacks*, such as virus, spyware, phishing, and spam email, that corporations face on the daily or even hourly basis. The probability of such distributed attacks overwhelms other types of security incidents (CSO 2005), but their consequences are generally limited. The *targeted attacks*, such as the purposeful penetration into the bank's systems to transfer large amount of money by hackers, constitute another class of security challenges. Such attacks may be less frequent than distributed attacks, but they tend to cause large damages to the targeted firms. For instance, per-respondent loss from "theft of proprietary information" is three times that from virus in the 2005 CSI/FBI survey (Gordon et al., 2005). Yet other classes, such as insider attacks and property theft, of security incidents exist. Firms may need to invest in different measures to defend against different classes of attacks, and economic analysis focusing on the optimal *allocation* of information security investment to each of the classes can be helpful to decision makers. In the following section, we present a model for such a purpose.

## 3. Model Construction

We consider a single-period, multi-event model for information system security of a firm (see Figure 1 for a conceptual description of the model). Threat agents, which can be external or internal to the firm, generate attacks on the information systems. Some of the attacks compromise the security of the information systems (with the breach probability $\rho$) cause damages (of the potential loss L) to the firm. The security risk $z$ the firm faces can therefore be written as (Kaas et al., 2001, Schechter 2004)

$$z = \rho \mathrm{L} . \tag{1}$$

The breach probability $\rho$ is a function of the behavior of the attack agents, characterized by their attack probability $\xi$, and the security property of the information systems, which is in turn determined by the system vulnerability and security measures. For any given system, the higher the attack probability, the higher breach probability; that is, $\partial\rho/\partial\xi \geq 0$. The system vulnerability, $v$, is intrinsic to the topology and connectivity of the firm's information systems: the more access and connected the systems, the more intrinsically vulnerable. In other words, $v$ represents the probability ($0 \leq v \leq 1$) for a security breach *without any additional security investment*. The breach probability is an increasing function of $v$; that is, $\partial\rho/\partial v \geq 0$. It is important to note that, in this definition, the system's configuration, access, and connectivity are dictated by the firm's business requirements, not technology choices. So, for instance, the firm in question may choose to allow its vendors to access certain areas of its information systems, a decision which may facilitate its business operations but would increase the vulnerability. To protect against the system vulnerability being exploited by threat agents, the firm invest $S$ in security measures. This investment can take many forms, from technologies such as firewalls and anti-virus software, to procedures such as auto log-off and password aging, to policies such as user training and security audits. We require that the effect of the security investment is a reduction of breach probability, or

$$\frac{\partial\rho}{\partial S} \leq 0 . \tag{2}$$

We further assume that this reduction is governed by the law of diminishing return, which implies that

$$\frac{\partial^2 \rho}{\partial S^2} \geq 0 . \tag{3}$$

To summarize, the breach probability can be described as

$$\rho = \rho(\xi, v, S) , \tag{4}$$

subject to the boundary condition

$$\rho^0 = \rho(\xi, v, 0) = \xi v . \tag{5}$$

Now we consider the case of *n* types of simultaneous attacks. We assume that each type of attack can be described by its own breach probability and loss. In other words,

$$z_i = \rho_i \mathrm{L}_i , \forall i \in [1, n] \bigcap I , \tag{6}$$

where $\rho_i = \rho_i(\xi_i, v, S_i)$. Note that the vulnerability *v* is the same for all attacks, because it is intrinsic to the systems. $\mathrm{L}_i$ represents the potential economic (i.e., monetary) loss the firm faces when the $i^{\text{th}}$ type of attack happens. This loss can be the direct—for instance, stolen product information—or indirect—for instance, customer losing trust of a company that could not safeguard credit card data—result of security breach of this particular type of attack. Without loss of generality, we make the simplifying assumption that each $\mathrm{L}_i > 0$ is a fixed amount, as estimated by the firm based on the type of attack. We further assume that $\mathrm{L}_i$ can be very large but always remains finite; that is, our model does not cover the case of potential losses of a catastrophic level. So in the case of a firm facing *n* types of attacks, the total information security risk can be expressed as

$$Z = \sum_{i=1}^{n} z_i = \sum_{i=1}^{n} \rho_i (\xi_i, v, S_i) \mathrm{L}_i . \tag{7}$$

To protect against the $i^{\text{th}}$ type of attack, the firm makes investment $S_i$ to reduces the breach probability $\rho_i$, hence, from (5) and (6), reducing the information security risks that the firm faces by $\Delta z_i = (\rho_i^0 - \rho_i)\mathrm{L}_i = (\xi_i v - \rho_i)\mathrm{L}_i$. If the firm repeats the same process for all $n$ types of attacks, the net benefit of all the security investments of $S_i$, $i = 1..n$, can be expressed as

$$\begin{aligned}\Phi(S_1,..,S_n) &= \sum_{i=1}^{n}(\Delta z_i - S_i) \\ &= \sum_{i=1}^{n}(\xi_i v - \rho_i)\mathrm{L}_i - \sum_{i=1}^{n} S_i\end{aligned}, \quad (8)$$

And it is subject to the boundary condition the marginal net benefit of any security investment $S_i$ at $S_i = 0$ is non-negative; in other words, the initial security investment of $S_i$ has to produce non-negative net benefit. Mathematically, this condition is written as

$$\frac{\partial \Phi}{\partial S_i}(S_1,..,S_i = 0,..,S_n) \geq 0, \forall i = 1,..,n. \quad (9)$$

The task of optimizing the security investments is to maximize their benefits Φ.[1] In later sections, this optimization is performed by setting the first-order partial differentiation of $\Phi(S_1,..,S_n)$ in (8) with respect to each $S_i$; that is $\partial\Phi / \partial S_i = 0$. And this operation indeed yields maximum, not minimum, of Φ:

$$\frac{\partial^2 \Phi}{\partial S_i^2} = -\frac{\partial^2 \rho}{\partial S_i^2}\mathrm{L}_i \leq 0, \quad (10)$$

because $\partial^2 \rho / \partial S_i{}^2 \geq 0$, $\forall i$, from (3).

[1] We follow Gordon and Loeb (2002) in making the assumption of a risk-neutral firm. When the decision-maker of a firm is risk-neutral, he is said to be indifferent towards investment decisions that carry the same expected values, even when they assume different risks (that is, different probability of realization). In general, the attitude towards risk can be captured by the functional form of the utility function $u(w)$. For a discussion of optimal investment in information security by a risk-averse decision maker, see Huang et al. (2005b).

Without loss of generality, we consider the case of $n$ = 2, or two simultaneous attacks. We can then rewrite (8) to

$$\Phi(S_1, S_2) = (\xi_1 v - \rho_1)\mathrm{L}_1 + (\xi_2 v - \rho_2)\mathrm{L}_2 - (S_1 + S_2)\,. \tag{11}$$

For the two types of attacks, we adopt the two broad classes of security breach probability first proposed by Gordon and Loeb (2002):

$$\rho_1 = \frac{\xi v}{\kappa_1 S_1 + 1}, \tag{12}$$

$$\rho_2 = \xi v^{\kappa_2 S_2 + 1}\,. \tag{13}$$

$S_1$ and $S_2$ represent security investments made to counter Class 1 and Class 2 attacks, respectively, and the parameters $\kappa_1$ and $\kappa_2$ measure the level of impact of, or the return on, the security investment. For any given security investment $S$, the higher the $\kappa$, the more reduction of the breach probability. We further simplify it by assuming that $\xi_1 = \xi_2 = \xi$. The associated potential losses of the two classes are $\mathrm{L}_1$ and $\mathrm{L}_2$. The total security investment that the firm makes in the case of two simultaneous attacks is the sum of the investments made to counter the individual attacks:

$$S = S_1 + S_2. \tag{14}$$

Before we proceed, it is important to examine these two classes of attacks based on the property of the breach probabilities. $\rho_1$ in (12) increases linearly with the system vulnerability, a characteristics generally exhibited by primary attacks such as one targeted at a firm's databases that store customer credit card information by exploiting specific system vulnerabilities. The Class 2 security breach probability in (13), which increases slowly at first with an increase in vulnerability but then rapidly when the vulnerability crosses a certain threshold (Figure 2), seems to appropriately describe mass or distributed attacks such as computer virus attack through email attachments. With respect to the security investment, Class 2 probability is much more convex in *S* than Class 1 (Figure 3), meaning that an initial investment in security is likely to have a more significant impact on the security threats represented by $\rho_2$ than those represented by $\rho_1$. This comparison fits well with the response to security investment by the reduction of breach probability from distributed attacks verses that from targeted attacks, because it is often more difficult to stop a determined attacker who tries to break into a particular system with known or unknown vulnerabilities. Based on these characteristics, we posit that that Class 1 in (12) best describes a targeted attack, while Class 2 in (13) can be regarded as that related to a mass or distributed attack (Huang et al., 2005).

Substituting (12) and (13) into (11) and rearrange the terms, we have

$$\Phi(S_1, S_2) = \frac{\xi v \kappa_1 S_1 \mathrm{L}_1}{\kappa_1 S_1 + 1} + \xi v (1 - v^{\kappa_2 S_2}) \mathrm{L}_2 - (S_1 + S_2). \tag{15}$$

Maximizing the total net benefit Φ in (15) then yields the optimal security investments for both classes of attacks. In the following sections, we examine several models, each with different assumptions and constraints, to arrive at the optimal level of security investments $S_1$ and $S_2$.

## 4. Independent Investments without Constraints

Our first model concerns with the situation where the firm evaluates investment for each type separately with no budget constraint, and security measures deploy to combat Class 1 attacks do not have any effects on Class 2 attacks and vice versa. In other words, the decision on and the impact of investments $S_1$ and $S_2$ are completely independent of each other. We first apply (9) to $S_1$ and $S_2$ in (15) independently to produce the following boundary conditions:

$$\frac{\partial \Phi}{\partial S_1}(0, S_2) \geq 0 \Rightarrow v \geq \frac{1}{\xi \kappa_1 \mathrm{L}_1}; \tag{16}$$

$$\frac{\partial \Phi}{\partial S_2}(S_1,0) \geq 0 \Rightarrow -v \ln v \leq \frac{1}{\xi \kappa_2 \mathrm{L}_2}. \tag{17}$$

In this case, we solve for optimal investments for Class 1 and Class 2 by taking the partial derivative of (15) with respect to one while holding the other constant:

$$\left.\frac{\partial \Phi}{\partial S_1}(S_1^*, S_2)\right|_{S_2} = 0, \tag{18}$$

and

$$\left.\frac{\partial \Phi}{\partial S_2}(S_1, S_2^*)\right|_{S_1} = 0. \tag{19}$$

These two first order conditions yield the optimal investments $S_1$* and $S_2$*. With (14), we get

$$S^* = \frac{\sqrt{\xi v \kappa_1 \mathrm{L}_1} - 1}{\kappa_1} + \left(\frac{1}{\kappa_2 \ln v}\right) \ln\left(-\frac{1}{\xi \kappa_2 \mathrm{L}_2 v \ln v}\right). \tag{20}$$

A quick comparison between (16) and the individual optimization based on Class 1 and Class 2 attack alone (equations (6) and (8) in Gordon and Loeb, 2002) shows that the *S** in this case is the straight sum of the optimal investments obtained by optimizing the utility function with respect to individual attacks separately, which is to be expected. Equation (20) is plotted in Figure 4.

From boundary condition (16), we notice that there exists a lower bound of *v* for finding *S**. However, in the case of $\mathrm{L}_1 > \mathrm{L}_2$, this *v* lower bound can be very small with large $\mathrm{L}_1$. Further, the optimal investment does not strictly increase with vulnerability. *S** increases with *v* initially, starts to drop after certain *v*, and eventually becomes an strictly increasing function of *v* when *v* is large. To summarize, the optimal total investment *S** in information security in the case of simultaneous attack, with no additional constraints, becomes nonzero above some minimum vulnerability *v* and increases with *v* thereafter. When *v* becomes large, *S** starts to drop, but eventually becomes a strictly increasing function of *v*.

## 5. Independent Investments with Budgetary Constraint

Equation (20) gives the optimal level when the firm makes decisions on how much to investment to protect its information systems from two classes of independent but simultaneous attacks. Ideally the investments would be solely determined by system parameters such as *v*, *ξ*, and L. In reality, however, a firm's ability to invest in information security, or anything else for that matter, is limited by its budget. That is, a firm may not be able to make certain level of security investment even when it was deemed optimal economically. Faced with a budgetary requirement, the firm then has to decide how much of the total security budget to *allocate* to Class 1 or Class 2 attack. The total investment thus becomes a constraint that represents the budgetary requirement, instead of a dependent variable (as in (20) and Figure 4). In this section, we examine the optimal allocation of information security investment among two classes of simultaneous attacks in the existence of such budgetary constraint.

### 5.1. The Model

Assume that the firm has set the total security investment to a fixed amount S. It follows that $S_1 + S_2 = \mathrm{S}$, no matter what the threat or vulnerability levels are. In other words, $S_1$ and $S_2$ are no longer independent of each other. In this case, we rewrite $\rho_2$ in (13) into a function of $S_1$ by noting that $S_2 = \mathrm{S} - S_1$:

$$\rho_2(S_1) = \xi v^{\kappa_2(\mathrm{S}-S_1)+1} = \xi v^{\kappa_2 \mathrm{S}+1} v^{-\kappa_2 S_1} . \qquad (21)$$

And we also have [2]

$$\frac{\partial \rho_2}{\partial S_1} = -\kappa_2 \ln v \xi v^{\kappa_2 \mathrm{S}+1} v^{-\kappa_2 S_1} \tag{22}$$

and

$$\frac{\partial^2 \rho_2}{\partial {S_1}^2} = {\kappa_2}^2 (\ln v)^2 \xi v^{\kappa_2 \mathrm{S}+1} v^{-\kappa_2 S_1} . \tag{23}$$

Substituting (14) and (21) into (11), we get

$$\Phi(S_1) = \frac{\xi v \kappa_1 S_1 \mathrm{L}_1}{\kappa_1 S_1 + 1} + \xi v (1 - v^{\kappa_2 \mathrm{S} - \kappa_2 S_1}) \mathrm{L}_2 - \mathrm{S}. \tag{24}$$

Differentiating $\Phi(S_1)$ with respect to $S_1$, we get

$$\begin{aligned} \left.\frac{\partial \Phi}{\partial S_1}\right|_{\mathrm{S},\mathrm{L}_1,\mathrm{L}_2,v,\xi} &= -\frac{\partial \rho_1}{\partial S_1}\mathrm{L}_1 - \frac{\partial \rho_2}{\partial S_1}\mathrm{L}_2 \\ &= \frac{\xi \kappa_1 v \mathrm{L}_1}{(\kappa_1 S_1 + 1)^2} + \xi \kappa_2 \ln v \mathrm{L}_2 v^{\kappa_2 \mathrm{S}+1} v^{-\kappa_2 S_1} \end{aligned} , \tag{25}$$

The boundary condition (9) requires that (25) is equal to or greater than zero when $S_1 = 0$. After rearranging terms, we get

$$-\frac{\mathrm{L}_2}{\mathrm{L}_1}\frac{\kappa_2}{\kappa_1}(\ln v) v^{\kappa_2 \mathrm{S}} \le 1 . \tag{26}$$

And this leads to the following (proof is omitted):

> *Corollary 1. In the case of independent investments to counter the attacks as described by the two breach probability functions (12) and (13), the total budget constraint has a lower bound* $\mathrm{S}_0 = \frac{1}{\kappa_2 \ln v} \ln\left( -\frac{\mathrm{L}_1}{\mathrm{L}_2}\frac{\kappa_1}{\kappa_2}\frac{1}{\ln v} \right)$ *when* $v < v' = e^{-\frac{L_1}{L_2}\frac{\kappa_1}{\kappa_2}}$.

[2] (23) is always non-negative, because $\ln v$ is negative for all $v \in [0,1]$. Note that, however, this does not violate the condition for breach probability (3), because when $S_1$ increases, $S_2$ actually decreases due to the fixed budget S, so ${\partial \rho_2}/{\partial S_2} \le 0$ still holds.

To find the optimal investment *S₁** (and *S₂** is therefore determined), we set (25) to zero. After rearranging terms, we get the following equation:

$$\frac{v^{\kappa_2 S_1 *}}{(\kappa_1 S_1^* + 1)^2} = -\frac{\mathrm{L}_2}{\mathrm{L}_1}\frac{\kappa_2}{\kappa_1}(\ln v)v^{\kappa_2 \mathrm{S}}. \tag{27}$$

We first note that (27) indeed yields the maximum of Φ($S_1$), because both ${\partial^2 \rho_1}\big/{\partial S_1{}^2} \geq 0$ (from (3)) and ${\partial^2 \rho_2}\big/{\partial S_1{}^2} \geq 0$ (form (23)),

$$\frac{\partial^2 \Phi}{\partial S^2{}_1} = -\frac{\partial^2 \rho_1}{\partial S_1{}^2}\mathrm{L}_1 - \frac{\partial^2 \rho_2}{\partial S_1{}^2}\mathrm{L}_2 \leq 0. \tag{28}$$

We also note that the boundary condition (26) holds for (27), because the left-hand side of (27) is always smaller than or equal to one: $v^{\kappa_2 S_1 *} \leq 1$ (since $v \in [0, 1]$) and $(\kappa_1 S_1^* + 1)^2 \geq 1$, for all $S_1$* > 0. A close examination shows that a closed-form $S_1$* cannot be obtained from (27), but some analyses of the absolute value of $S_1$* can be done without such a solution. When S increases, the right hand side of (27) decreases (since $-\frac{\mathrm{L}_2}{\mathrm{L}_1}\frac{\kappa_2}{\kappa_1}(\ln v)$ > 0), giving rise to a larger $S_1$* in the left hand side, which is a strictly decreasing function of $S_1$* for all $S_1$* > 0 (since $v \in [0, 1]$). That is, when the total budget S increases, so does the optimal investment $S_1$*. Further, since ln*v* < 0,

$$\frac{v^{\kappa_2 S_1 *}}{(\kappa_1 S_1^* + 1)^2} \propto \frac{\mathrm{L}_2}{\mathrm{L}_1}. \tag{29}$$

And because, again, the left hand side is a decreasing function $S_1$*, we conclude that, from (29), $S_1$* increases with the ratio $\mathrm{L}_1/\mathrm{L}_2$. That is, optimal investment $S_1$* is higher when the potential loss $\mathrm{L}_1$ is higher relative to the potential loss $\mathrm{L}_2$. To summarize, when a firm faces two simultaneous attacks, the *absolute value* of the optimal security investment against one of the attacks increases with the total security budget, as well as with the increase of the relative potential loss of that attack to that of the other one.

### 5.2. Computational Results

Of particular interest in (27) is how the firm would *allocate* security investments given a budgetary constrain. Because no closed-form solution is possible, we use numerical analysis to examine the optimal investment allocation to Class 1 attack, as represented by $S_1$*/S (and allocation to Class 2 attack, $S_2$*/S, is thus determined). In this section, we compute and graph $S_1$*/S with respect to four parameters of interest, namely the total security budget S, the system vulnerability $v$, ratio of investment effectiveness $\kappa_1$ and $\kappa_2$, and the ratio of potential loss $L_1$ and $L_2$.

The first set of numerical analysis examines how $S_1$*/S varies with $v$, the intrinsic system vulnerability. We fix $\kappa_1$, $\kappa_2$, $L_1$, $L_2$, and S, and run a series of $v$ values to obtain the ratio $S_1$*/S. Figure 5 shows the result of $S_1$*/S vs. $v$ for three different sets of potential loss values ($L_1 = L_2 =$ \$2M; $L_1 =$ \$2M and $L_2 =$ \$1M; $L_1 =$ \$1M and $L_2 =$ \$2M), while fixing $\kappa_1 = \kappa_2 = 0.000005$ and S = \$100,000 (as 5% of either $L_1$ or $L_2$). We can see that, for each combination of $L_1$ and $L_2$, $S_1$*/S increases with $v$ between a minimum $v$ where $S_1$* remains zero and a maximum $v$ where $S_1$*/S approaches 100%. Further, the relative size of $L_1$ shifts the curve to the left.

The computational result in Figure 5 is readily understood when compared with the result of the single-event model presented by Gordon and Loeb (2002) as well as the independent model in Section 4. When attacks are considered separately, optimized investment for Class 1 starts at a higher $v$ than that for Class 2. However, the latter drops off to zero when $v$ gets large, while the former continues to increase with $v$. Therefore, when the total investment is fixed, the optimal allocation would shifts gradually from Class 2 to Class 1 with increasing vulnerability. And when Class 1 attack takes on more importance (as represented by the relative size of $L_1$ vs. $L_2$), this shift from Class 2 to Class 1 happens at a lower $v$ (thus covering a broader range of $v$). As a summary, when a firm faces two simultaneous attacks with a fixed total security investment budget, the firm should optimally allocate all of its investment to Class 2 when the system vulnerability is low, gradually increases, and eventually allocates all, its investment to Class 1. With larger potential loss due to Class 1 attack vs. that from the Class 2 attack, the range of vulnerability where the optimal investment allocated to the former is wider (i.e., starts at a smaller vulnerability).

Next, we examine how $S_1$*/S varies with $L_1/L_2$, by fixing S, $v$, $\kappa_1$, and $\kappa_2$. Figure 6 shows the result of one such set of computation, where we fix $\kappa_1 = \kappa_2 = 0.000005$, $v = 0.4$, and $L_1$ = \$2M while recording the relationship $S_1$*/S vs. $L_1/L_2$ by varying $L_2$ for S = \$100,000 (5% of $L_1$) and S = \$500,000 (12.5% of $L_1$). The result confirms the observation in Section 5.1 that $S_1$* increases with the ratio $L_1/L_2$ for a fixed S.

We further note that for the curve with small S (S=5% of $L_1$), $S_1$* starts to become non-zero when $L_1$ is about half of $L_2$ and takes all of the budget S when $L_1$ reaches twice as much as $L_2$. The curve of larger S (S = 12.5% of $L_1$), on the other hand, is smoother and over a larger range of $L_1/L_2$. In other words, the shift of allocation from investing against one class of attack to the other occurs at a higher relative loss and increases faster when the total budget is smaller.

Our next numerical analysis focuses on how the effectiveness of security investment, represented by $\kappa_1$ and $\kappa_2$, affects the allocation of investment. This is done by leaving all other parameters (S, $L_1/L_2$, and $v$) constant while varying $\kappa_1/\kappa_2$. Figure 7 shows the result of this calculation for $L_1 = L_2$ = \$2M, $v = 0.4$, and S = \$100,000 (5% of L) and S = \$500,000 (12.5% of

L). Initially, allocation to Class I (as represented by $S_1$*/S) increases quickly with $\kappa_1/\kappa_2$; that is, $S_1$*'s share of the total investment grows as the effectiveness of $S_1$ in reducing $\rho_1$ vs. $S_2$'s effectiveness in reducing $\rho_2$ increases. However, after $\kappa_1/\kappa_2$ reaches certain level, the share of $S_1$* starts to decrease, albeit slowly. In other words, when a firm invests a fixed amount of budget against two simultaneous attacks, allocation to investing in protecting against one class of attack increases with the effectiveness of such investment vs. that of the investment in the other class. When the relative effectiveness reaches a certain level, however, the allocation of investment starts to shift towards the less effective class.

This result can be interpreted as follows. Initially, when $\kappa_1/\kappa_2$ is very small, investing in measures against Class 1 attack is simply too ineffective, resulting in a zero allocation to it. $S_1$* starts to become positive after certain level of $\kappa_1/\kappa_2$; with increasing $\kappa_1/\kappa_2$, the optimal allocation to $S_1$* increases to capture the increasing relative effectiveness of investment in Class 1. Here, similar to the case of $S_1$*/S vs. $L_1/L_2$ for the reason of investment efficiency, the minimum level of $\kappa_1/\kappa_2$ for $S_1$* to become nonzero and the rate of increase thereafter are higher for small S. As $\kappa_1/\kappa_2$ crosses certain level, $S_1$* starts to decrease with increasing $\kappa_1/\kappa_2$, signaling that the gain in increasing effectiveness has peaked. When this happens, the optimal allocation starts to shift more towards Class 2.

Our last, but arguably the most interesting, analysis is focused on the optimal allocation among $S_1$* and $S_2$* at different levels of budgetary constraint S. From Section 5.1, we know that $S_1$* increases with S. A quick glance at (27) leads one to suspect that when the total security budget S goes up, the optimal *allocation* to Class 1 attack also increases: For a fixed $-\frac{L_2}{L_1}\frac{\kappa_2}{\kappa_1}(\ln v)$, the rate of increase of $S_1$* is higher than the rate of increase of S, because the value of the left hand side of (27) is offset by the denominator $(\kappa_1 S_1^* + 1)^2$ for all $S_1$* > 0.

However, this observation may not hold true for all S at varied combinations of all other parameters, in particular $v$, $\kappa_1$, and $\kappa_2$, because of the presence of S in the exponent on the right hand side as well as the boundary condition (26). We therefore perform numerical analysis on (27) to uncover the effect of the budgetary constrain S on the optimal allocation to $S_1$*.

Two sets of the computational results are presented in Figures 8 and 9, where $S_1$*/S, the optimal allocation to Class 1 attack, is plotted against S/L$_1$, the "normalized" budget constraint, in a family of "iso-vulnerability" curves. In Figure 8, with $\kappa_1$ = 0.000003, $\kappa_2$ = 0.000005, L$_1$ = \$2M, and L$_2$ = \$3M, those curves are all concave and increasing, implying that the percentage allocated to $S_1$* increases, albeit at a decreasing rate, with S. Also, both the value and the slope of $S_1$*/S is higher for larger $v$, implying that the allocation to $S_1$* increases with $v$ for any given S. These results are consistent with both the above observation of (27) and earlier result with respect to $v$. However, Figure 9, where we set $\kappa_1$ = $\kappa_2$ = 0.000005 and L$_1$ = L$_2$ = \$2M, shows a distinctively different behavior of $S_1$*/S vs. S/L$_1$. At small $v$, the iso-vulnerability curves are concave and increasing, similarly to those in Figure 6. When $v$ become sufficiently large, however, the iso-vulnerability curves become U-shape. That is, for $v$ greater than some "inflection point" $v'$, $S_1$*/S is convex and non-increasing in S/L$_1$: at small S, $S_1$*'s share *decreases* with increasing total investment, and approaches 100% when S → 0; for large S, optimal allocation $S_1$* *increases* with the total investment, and approaches 100% when S becomes large. And throughout all levels of total investment, $S_1$*'s share never approaches 0.

From the modeling perspective, the distinctive behavior can be partially explained by Corollary 1. For any given $\kappa_1$, $\kappa_2$, L$_1$, and L$_2$, S has a lower bound when $v < v' = e^{-\frac{L_1}{L_2}\frac{\kappa_1}{\kappa_2}}$, hence the lower curves in Figure 9. When $v > v'$, S no longer has lower limit, and the curves cover the whole range of S. ( $v' = e^{-1} \cong 0.3678$ in Figure 9.) However, when $\frac{\mathrm{L}_2}{\mathrm{L}_1}\frac{\kappa_2}{\kappa_1}$ becomes large enough such that $v' = e^{-\frac{L_1}{L_2}\frac{\kappa_1}{\kappa_2}} > 1$, the lower bound $S_0$ exists for all $v \in [0,1]$, and all the iso-vulnerability curves behave like those in Figure 8. In summary, our computational result shows that under most circumstances (e.g., Figure 8 and part of Figure 9), the optimal allocation to Class 1 increases with total security budget. However, when the potential loss from Class 1 attack is sufficiently small compared to that from the Class 2 attack, and when the system vulnerability is sufficiently large, optimal allocation to protecting against Class 1 attack approaches 100% when the total investment constraint is very small, decreases and then increases with increasing S, and approaches 100% with large budgetary constraint.

## 6. Discussions and Conclusions

So far, the analyses have been strictly based on the mathematic properties of the models. In the section, we attempt to link the modeling results to practice, hoping to gain insight into the management of information security investment.

In the case of independent investments with no budgetary constraints, our analysis shows two interesting characteristics. First, there exists a minimum vulnerability below which investment is zero. This tolerance threshold for not investing is much lower, as can be expected, when breaches from targeted attacks would cause large losses. The second characteristic is the drop in total investment beyond a specific vulnerability. In practice, beyond this level of vulnerability, it may be more beneficial for the firm to concentrate on recovery from the losses (such as maintaining system integrity, ensuring business continuance or mitigating liability incurred) than on investment to defend against vulnerability.

When the total budget is limited, the *absolute* level of investment to protect against a specific type of attack increases as the potential loss from type of attack increases or when the total budget increases. This is an expected reaction. And when we consider the relative loss between targeted and distributed attacks, we find that firms could start shifting investment *allocation* from protecting against distributed attacks to protecting against targeted attacks as the loss associated with the latter increases. As can be expected, such shifts begin to occur at lower vulnerabilities when the losses from targeted attacks are greater. This can be interpreted as simply a case of placing more investment to protect against the greater loss. The interesting outcome of the analysis, however, is that the fixed budget can very quickly get absorbed in protecting against targeted attacks with slight increases in vulnerability, exposing the firm to distributed attacks with non-zero potential losses. Further, when the total investment is small, the shift of allocation from protecting against one threat to another is quicker. This result can be understood from the perspective of the effective use of investment: When the total budget is small, it may be better off for the firm to concentrate the investment in one class of attack when the other class poses relative low risks (i.e., when $L_1/L_2$ is small); but when the latter does impose enough threat (as demonstrated by large enough $L_1/L_2$) to justify a diversion of funds from the first one, allocation goes up quickly, because a small portion of the already small total may not produce much effect.

We also find that the investment allocation to securing against targeted attacks increases with an increase in the relative effectiveness of that investment. This is a reasonable response in any firm. However, our analysis also shows that beyond a certain level of increased relative effectiveness, allocation of investment in that category peaks and then reduces relative to the allocation in the other category, implying that investment in the former is so effective that less allocation is needed to achieve some required level of security. It is also interesting to note that for smaller total budgets, the peak allocation for protecting against targeted attacks occurs at a higher relative effectiveness and a greater share of total budget. This result can signal the presence of a critical mass of investment for protecting against targeted attacks, irrespective of the investment effectiveness.

The observation of the optimal allocation with respect to the size of budget constraint has interesting practical implications. Under most circumstances, when a firm faces both distributed and targeted attacks, the percentage allocated to protecting against the latter goes up with increasing security budget. This can be understood from the fact that distributed attacks are, in general, less sophisticated and stopped more effectively with relatively low amount of security investments. Thus, when the budget is small, it is more effective to allocate the bulk of it to distributed attacks; and with an increased security budget, more allocation would go to targeted attacks. However, when the potential loss from targeted attacks is sufficiently large, the firm with a large information systems vulnerability and a very small security budget would cast all security investments against targeted attacks. It would gradually reduce the allocation percentage with increasing budget, but eventually start increasing the allocation ultimately to 100%. When vulnerability is large, the risk from targeted attack is high and very real (due to high potential risk), and allocating the bulk of the security budget would make sense even when it is very small. And the budget becomes larger, distributed attack gets its own share of investment, and the allocation curve exhibits behavior common to other situations.

In this study, we analyze the security investment decision for a firm facing multiple attacks with the help of economic modeling. Our results, in particular, offer insights into how a decision maker should allocate security investment budget at various levels of systems vulnerability, relative potential loss, investment effectiveness, and total budget. As with all models, a number of assumptions are made to make our model manageable but may limit its applicability to practice. For instance, we follow a previous study in assuming that the firm is risk-neutral (Gordon and Loeb, 2002), while, in reality, many decision makers can be regarded risk-averse. Also, our model assumes that the security investments to counteract the two classes of attacks are independent of each other, while, in reality, security measures taken to prevent one class of attack may help prevent another class of attack. Future studies that relax these and other assumptions, as well as empirical verifications of the modeling results, can help advance this stream of research.

## References

AT&T (2004). Network security: Managing the risk and opportunity. *AT&T Point of View*, July 2004, 1-21.

Carr, N. G. (2003). IT Doesn’t Matter. *Harvard Business Review,* 81(5), 41 -49

CSO (2005). *2005 E-Crime Watch™ Survey: Summary of Findings*. Framingham, Mass.: CSO Magazine.

Fiegenbaum, A., and Thomas, H. (1988). Attitudes toward risk and the risk-return paradox: Prospect theory explanations. *Academy of Management Journal*, 32(1), 85-106.

Gordon, L.A., and Loeb, M.P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and Systems Security*, 5(4), 438-457.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., and Richardson, R. (2005). *2005 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute.

Huang, C.D., Hu, Q., and Behara, R. (2005a). In search for optimal level of information security investment in risk-averse firms. *Proceedings of the Third Annual Security Symposium*, Tempe, Arizona, September 8-9.

Huang, C.D., Hu, Q., and Behara, R. (2005b). Investment in information security by a risk-averse firm. *Proceedings of the 2005 Softwars Conference*, Las Vegas, Nevada, December 10-11.

Jegers, M. (1991). Prospect theory and the risk-return relation: Some Belgian evidence. *Academy of Management Journal*, 34(1), 215-225.

Kaas, R., Gavaerts, M., Phaene, J., and Dennit, M. (2001). *Modern Actuarial Risk Theory*, Boston, Mass.: Kluwer Academic Publishers.

Ogut, H., Menon, N., and Raghunathan, S. (2005). Cyber Insurance and IT security investment: Impact of interdependent risk. *Proceedings of the Workshop on the Economics of Information Security (WEIS05)*, Kennedy School of Government, Harvard University, Cambridge, Mass., June 2-3.

Power, R. (2003). 2003 Global Security Survey, Deloitte Touche Tohmatsu. Accessed on March 17, 2003, online at http://www.deloitte.com/dtt/cda/doc/content/Global%20Security%20Survey%202003.pdf

Schechter, S.E. (2005). Toward econometric models of the security risk from remote attacks. IEEE Security & Privacy, 3(1), 40-44.

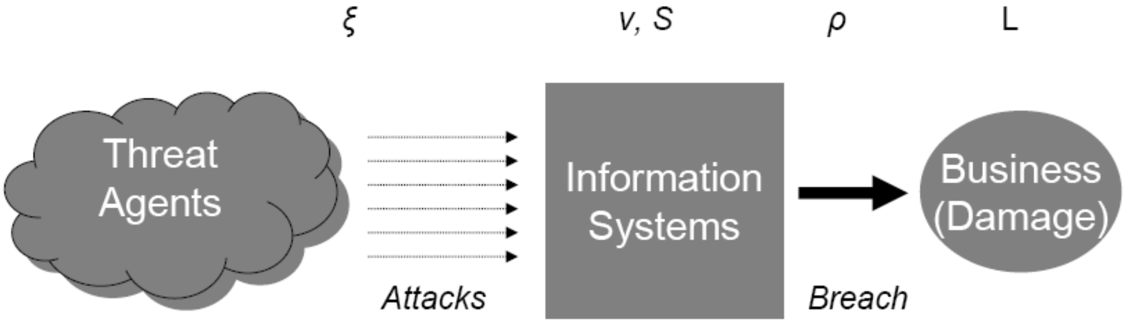

Figure 1. Information Security Model

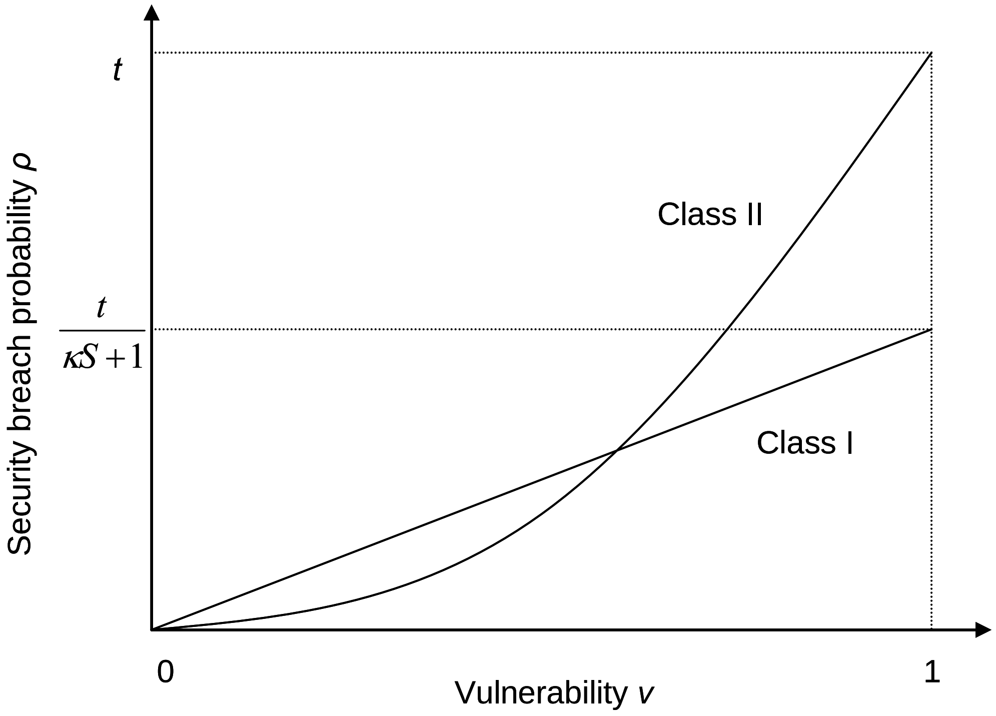

Figure 2. Security breach probability functions vs. *v*

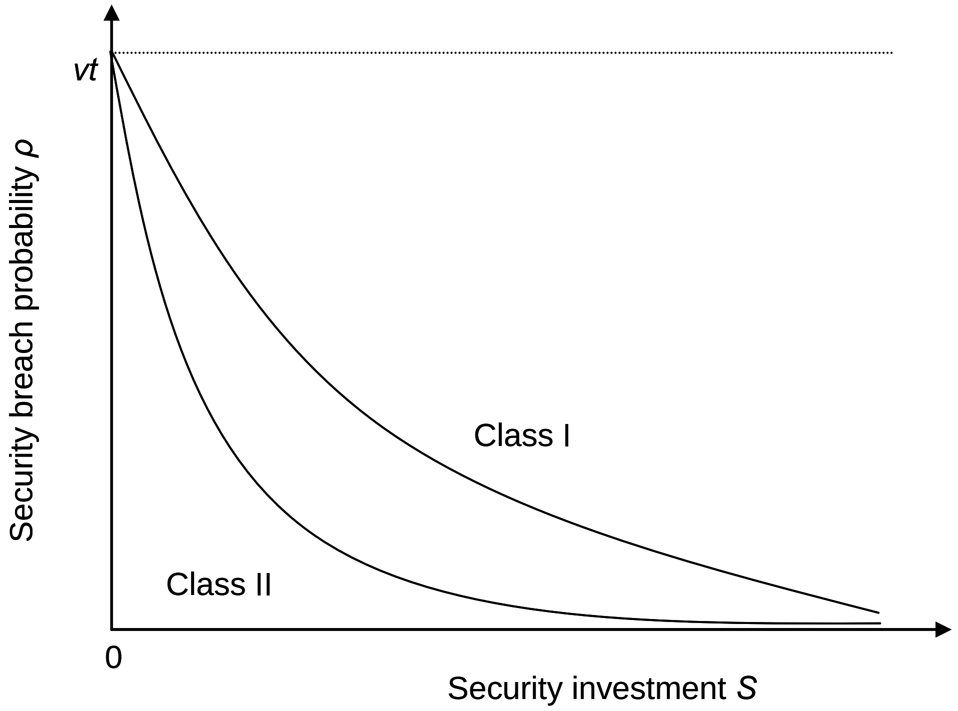

Figure 3. Security breach probability functions vs. *S*

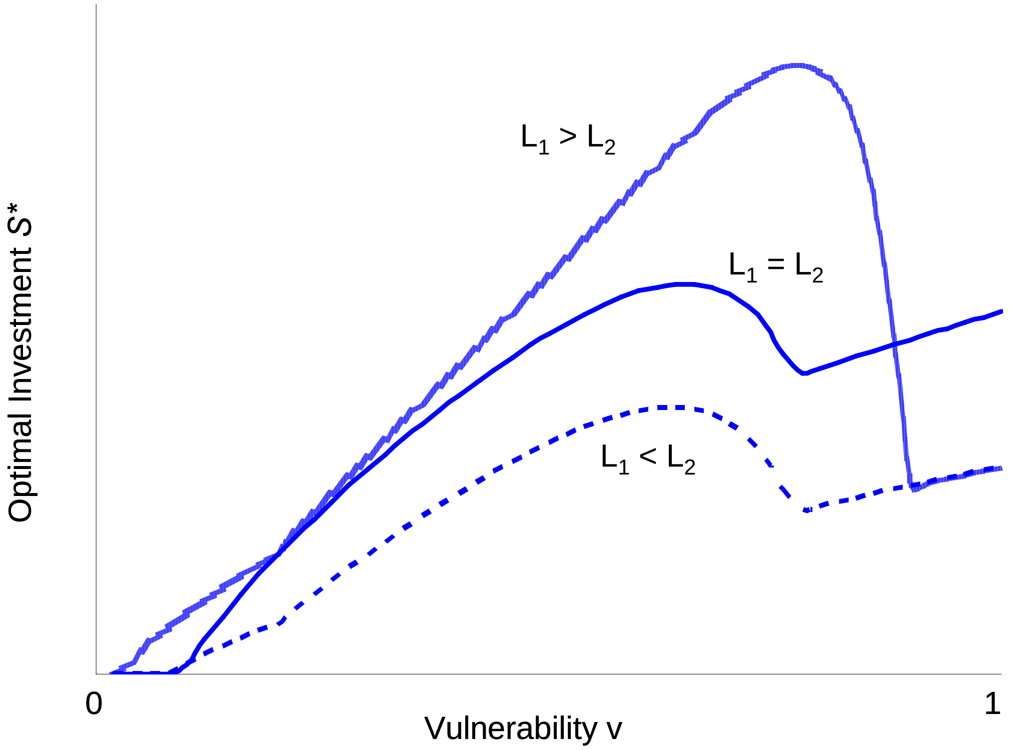

Figure 4. Optimal Information Security Investment vs. *v*, Independent Investments with No Additional Constraints

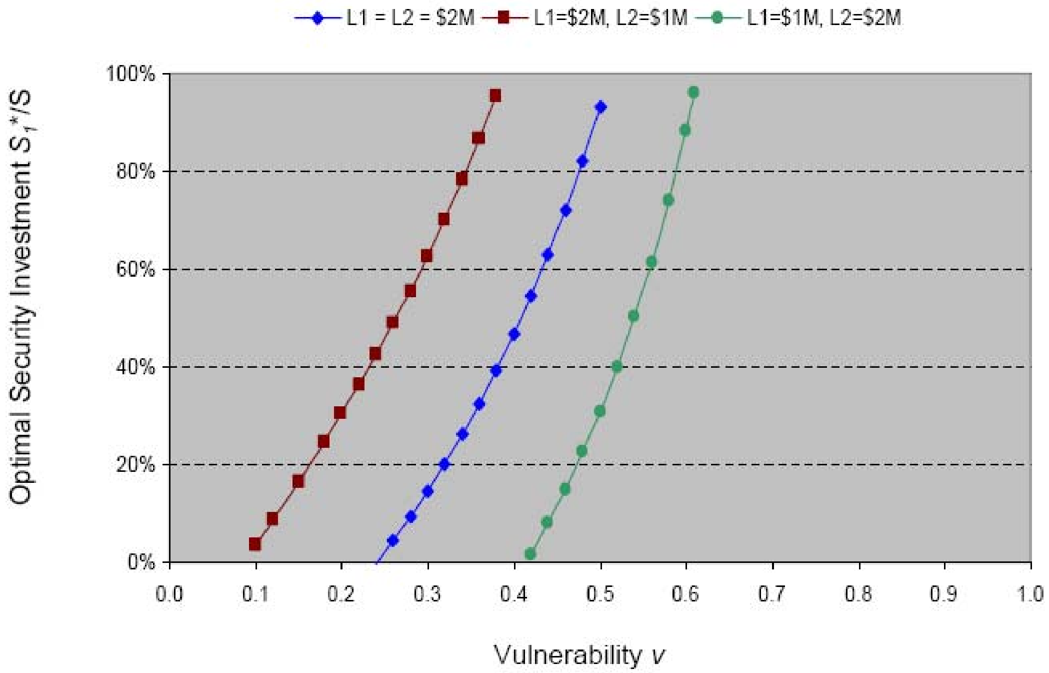

Figure 5. Optimal Information Security Investment allocated to $S_1$ vs. $v$, Independent Case with budget constraints

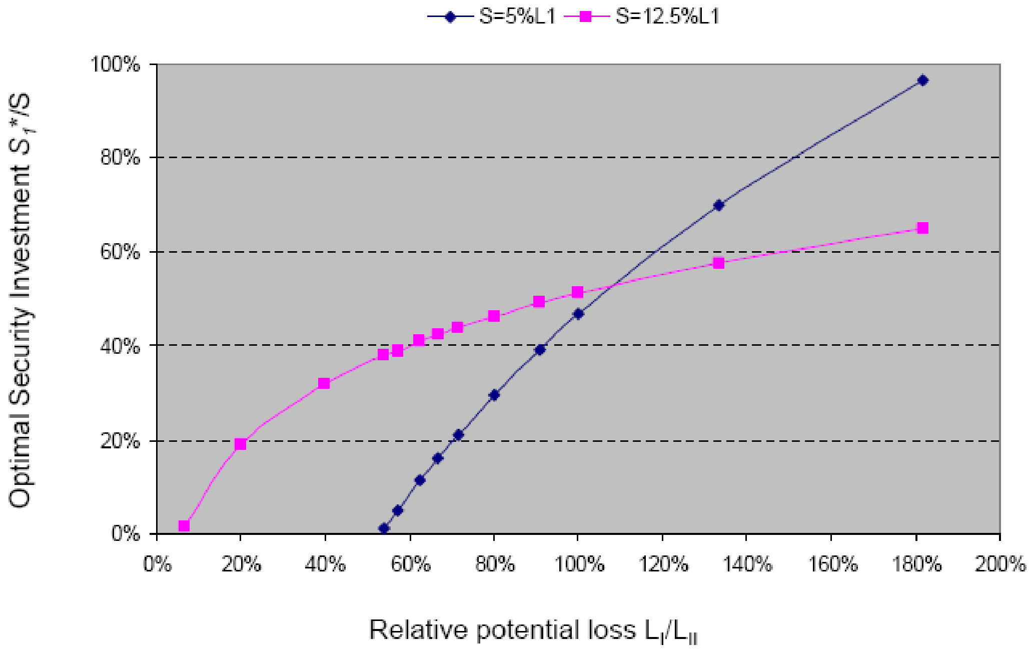

Figure 6. Optimal Information Security Investment allocated to $S_1$ vs. relative potential loss $L_1/L_2$, Independent Case with budget constraints

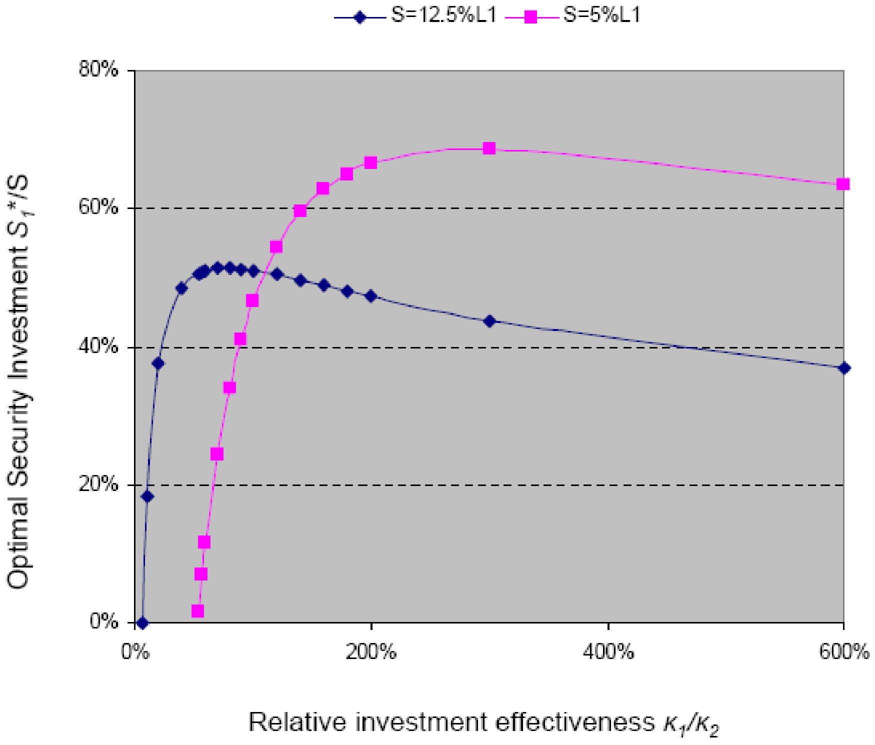

Figure 7. Optimal Information Security Investment allocated to $S_1$ vs. relative investment effectiveness $\kappa_1/\kappa_2$, Independent case with budget constraints

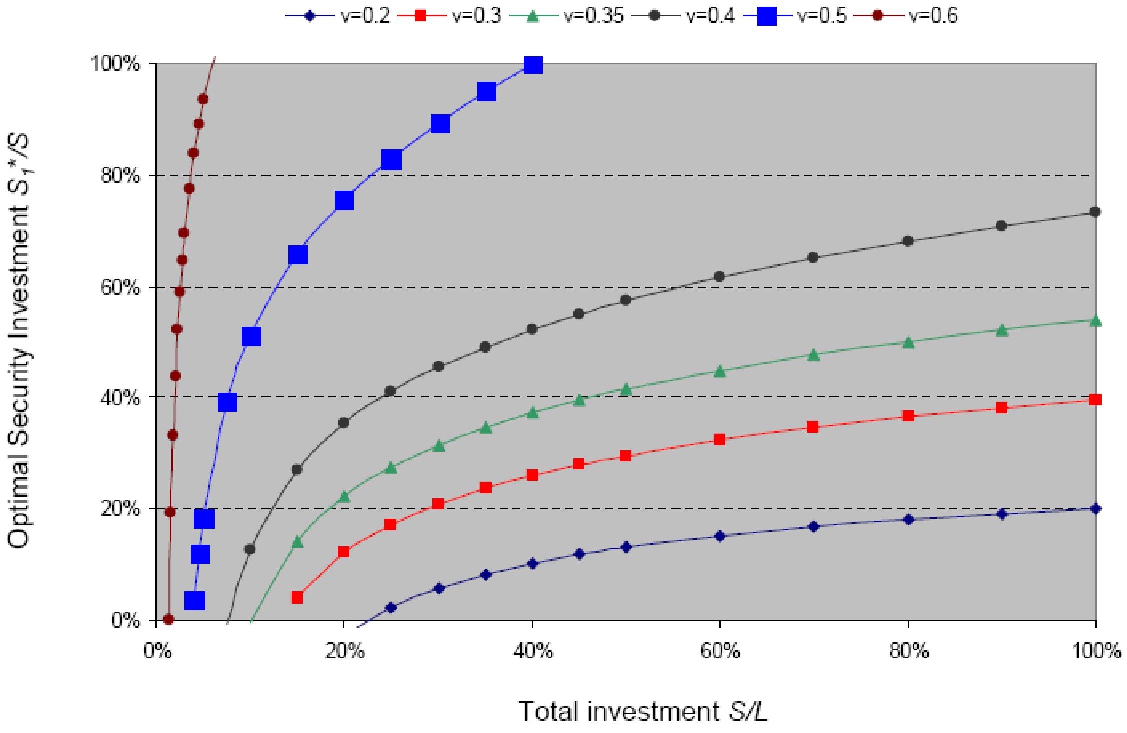

Figure 8. How budgetary constraint changes the optimal when everything else stays constant, independent case with budget constraints (parameter set #1)

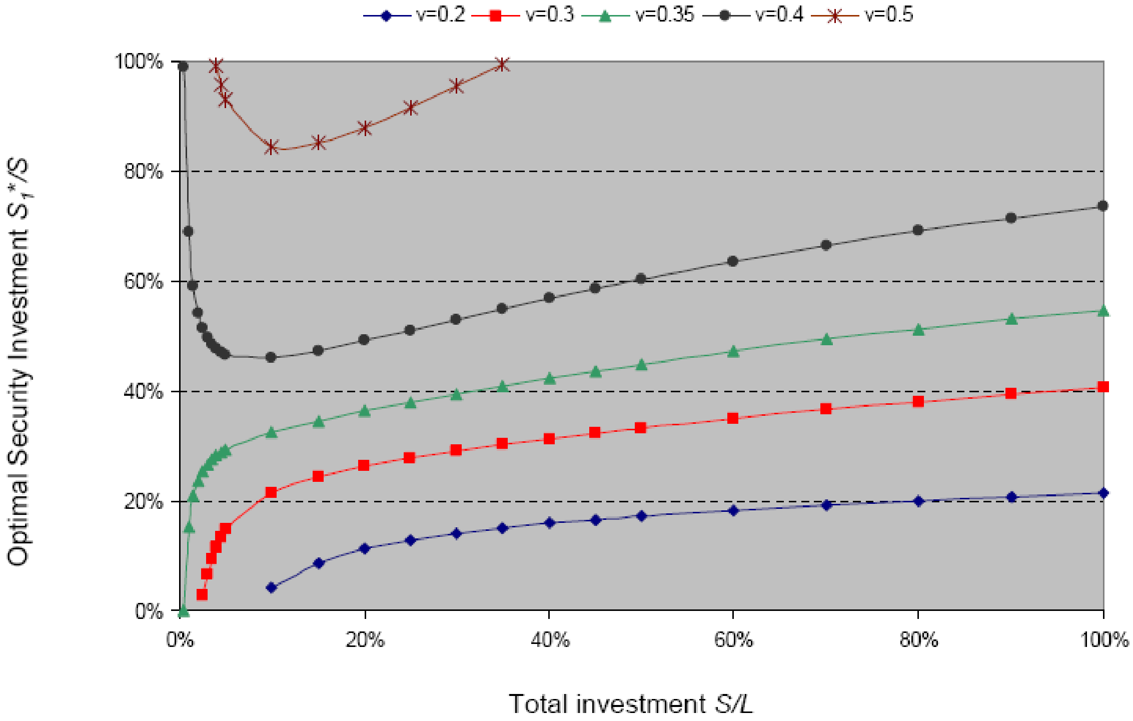

Figure 9. How budgetary constraint changes the optimal when everything else stays constant, independent case with budget constraints (parameter set #2)