http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.22, No.2, May 2017, pp.99-121
https://doi.org/10.7838/jsebs.2017.22.2.099

규제할 수 없는 보안통제가 존재하는 경우 보안 규제 설정

Security Standardization for Social Welfare in the Presence of Unverifiable Control

이철호(Chul Ho Lee)*

초 록

모든 영역에서 조직의 디지털 자산을 보호하기 위해, 보안 규제를 강제하고 있는 추세이다. 문제는 조직 내의 보안 통제장치 가운데 투입된 노력이나 보안 수준을 외부에서 확인할 수 없는 통제장치가 존재한다는 것이다. 이 논문에서는 확인할 수 없는 통제장치가 존재하는 경우, 합리적인 보안 수준이 무엇인지 불완전 계약이론을 적용하여 분석하였다. 이를 위해, 확인할 수 없는 통제장치를 무시하는 경우의 비이성적 규제(naive standard)와 모두 확인할 수 있다고 가정할 경우의 완전정보하의 규제와 비교 분석하였다. 결과는 통제장치의 구성에 따라 달라졌다. 우선 평형구성(parallel configuration)하에서는 완전정보하의 규제와 최적규제가 동일하였으며, 순차구성(serial configuration)하에서는 최적규제 수준이 낮아야 하며, 다른 비교대상 규제와는 차이를 보였다. 최적구성(best shot configuration)하에서 확인가능한 통제장치가 비용효율성이 높은 경우, 흥미롭게도 비합리적 규제가 최적규제수준과 동일한 것으로 나타났다.

ABSTRACT

Standard makers in both private and public sectors have been increasingly mandating security standards upon organizations to protect organizational digital assets. A major issue in security standardization is that standards often cannot regulate all possible security efforts by the standard maker because some efforts are unverifiable by nature. This paper studies from an analytical perspective how *a standard maker* should design the standard using a verifiable security control in the presence of another related unverifiable one. We compare it with two benchmark standards; *naïve-standard* which refers to the standard maker who ignores the existence of the unverifiable control, and *complete-information standard* which refers to the maker sets standards on both controls. Optimal standard and benchmark standard depend critically on how the two controls are configured. Under parallel configuration, the existence of the unverifiable control induces the policy maker to set a higher standard (the complete-information standard is optimal); under serial configuration, a lower standard is applied (neither benchmark works). Under best-shot configuration and if the verifiable control is more cost-efficient, the existence of the unverifiable control has no impact on the optimal standard (the naïve standard is optimal).

키워드 : 정보보안, 규제, 비규제성, 비이성적규제, 완전정보
Information Security, Standard, Unverifiability, Naïve Standard, Complete-Information

* Department of Business and Technology Management, College of Business Korea Advanced Institute of Science and Technology(irontigerlee@kaist.ac.kr)
Received: 2017-03-20, Review completed: 2017-03-30, Accepted: 2017-04-01

1. Introduction

With increasing connectivity, entities out of theorganizational boundary have been harmed from the breach of the organization's digital asset or online service. For instance, in 2005 the information system of a credit card processor, CardSystems Solutions, was breached and consequently 40 million credit card numbers were stolen [28, 35]. In this example, although the breach happened to a single company millions of consumers were affected-such an event caused polemic debates on whether organizations alone have enough motivation to invest adequately in information security especially when others (consumers in this case) shoulder the consequences of a breach. In this regard, standard makers in private as well as public sectors have been increasingly mandating information security standards upon organizations, not only to reduce the chance of damage from direct security breaches, but also to protect the value of all related stakeholders (such as an organization's supply chain partners and clients), whose private information is shared with these organizations. Two acknowledged prominent standard makers are PCI Security Standards Council and the National Institute of Standards and Technology (NIST). The first one mandates all merchants that use major payment cards (such as Visa and Master cards) in the private sector and the latter one regulates all US governmental agencies.

One major issue in security standardization is that standards cannot cover every possible security control of the organization because some controls are not verifiable to the standard maker. Such so-called unverifiability of security controls arise from a variety of reasons. First, some controls – especially including human diligence – are almost impossible to measure and trace even after the security breach occurred. For example, the effectiveness of a screening system at an airport aviationbureau (department) which critically depends on the professional judgment and prioritization ofthe IT security staff in charge thus such professionalism is hard to quantify. Additionally, it may be cost-prohibitive for standard makers to monitor the internal controls within any organization and to predict future potential attacks at the inception. Based on the latter, the following question may be raised: Will the existence of unverifiable security controls affect a standard maker's decision on the standards of verifiable security controls? If yes, how? To our knowledge, Lee et al. [20] is the only study pursuing an analysis on these highly relevant questions for practitioners. Our work is different from it in that this paper considers more configurations, best-shot configuration by investigating possible configuration in reality, and focuses on a standard maker's decision, and finally suggests highly practicable standards, naïve standard and complete information standard, for practitioners.

In an attempt to analyze the issue of security standardization under the presence of un-

verifiable security control, we built a game-theoretical model on Varian [33] work that considers two controls. The purpose of these two controls is to *jointly* pursue digital assets protection. For example, in order to enforce a sound password policy, a firm can use both, a password management software forcingemployees to pick long passwords which include special characters and at the same time IT security personnel to patrol the offices to detect and send warning messages to any employee who has handwritten password notes attached to her/his computer. The way these two security controls are connected to each other with regard to the digital asset protection is referred to as *security configurations*. It is depending on these configurations, that an attacker can cause damage to a digital asset either by breaching one or both controls. Based on these assumptions, we consider three basic and fundamental security configurations: *parallel, serial* and *best-shot* configurations.

We find that, with one exception, the answer to our first research question is affirmative. Even though a standard maker cannot directly mandate a firm's investment on the unverifiable security control, its standard on the verifiable control will *indirectly* affect the firm's incentive in terms of whether and how to invest on the unverifiable control, since the firm tries to strike an optimal balance between the two controls in order to protect the digital asset efficiently (from the firm's perspective). For that reason, in general it is not optimal for the standard maker to ignore the existence of any unverifiable security control when designing security standards. The only exception is for best-shot configuration and when the verifiable control is more cost-efficient than the unverifiable control – in such case, optimality calls for the firm to put all investment on the former control, thus the latter control becomes irrelevant.

We find that the extent and the way the existence of an unverifiable control will be affected by security standardization depends critically on the specific security configuration that the two controls are embedded in. Under parallel configuration, firm investment on the unverifiable security control increases in the standard of the verifiable control. Under best-shot configuration and if the verifiable control is relatively cost-efficient, the unverifiable control has no impact on the standard; nevertheless, if the unverifiable control is much more cost-efficient, the standard maker should not impose any standard at all, so the firm can make cost-efficient investment on the unverifiable control. In the case of serial configuration, firm investment on the unverifiable control decreases in the standard on the verifiable control. Consequently, the existence of the unverifiable control encourages the standard maker to set a lower standard.

The rest of the paper is organized as follows. In Section 2 we review relevant literatures. Wepresent our model in Section 3. We discuss three security configurations – parallel, best-shot and serial – in Section 4. Section 5 con-

cludes this paper.

2. Literature Review

While the existence of studies on security standards is sparse, we find relevant works from the literature of financial auditing standards. The works mainly show tougher standards hurts quality of service. Dye [9] first shows that the average quality of audits may decline with tougher auditing standards. Willekens et al. [34] states that the increased difficulty of dismissing a compliant auditor can decrease the quality of audit offered. Ewert and Wagenhofer [10] concluded that tighter accounting standards reduce earnings management, but can increase real earnings management because of self-interested motivation of the CEO. Our work is different from this line of studies since we considered multiple security controls and standard settings.

Our paper is also related to several seminal economic papers. Hendricks and McAfee [16] and Crawford [6] use a signaling model to analyze attacker-defender games. In our case, standards are established by a standard maker, and these signals could be used by attackers to compromise the defender's information asset. Bernheim and Whinston [3] reported that a complete contract may not be optimal in the presence of unverifiable performance.

Though security standards is a recent area of development as a strategy action to manage a determined ecosystem's security, the current studies on this topic are limited. Much of the work on this issue has taken a descriptive approach and focused on principles for standard governance [7, 18, 24, 27, 31]. Miller and Tucker [23], a paper focusing on the first step for the regulation's role, show that adoption of encryption software increases the incidence of publicized data losses because of carelessness about other protection activities. Hui et al. [17] show that a tougher standard can hurt a security ecosystem of firms in an outsourcing context. In the paper, the negative impact comes from implied security risks of shared security infrastructure. Our paper is closer to Lee et al. [20] in many aspects: the consideration of unverifiable controls and security configuration. However, Lee et al. [20] mainly focused on a firm's behavior in the presence of unverifiable control. This study showed how the unverifiable control affected the firm's security under different configuration settings, but the mentioned paper dealt with the standard maker's decision making process *numerically* due to a mathematical traceability issue. Nevertheless, our work shows the dynamics of security standardization with a much more simplified model, and adds other security control setting; best-shot configuration.

There have been diverse studies in the economics of IT security literature including optimal security investment, optimal security information sharing, and optimal contracting. Hausken [14] shows that the particular per-

formance structure matters when a firm decides its optimality on the security investment. Regarding information sharing, Gordon et al. [12] shows that the sharing of security information does not necessarily lead to better security because of free riding. Following these two studies, Hausken [14] advocates for an active role of social planners in the security information sharing. Regarding information security contracting, Dey [8] compare the performance of various outsourcing contracts and suggests optimal contract for the outsourcing. Recently, Lee et al. [13] showed that prevailing outsourcing contract in reality can enlarge the moral hazard problem with externality effects, and proposed an optimal solution to address the double moral hazard problem. Our research contributes to the information security literature by examining the role of security standards in incentivizing firm investments when not all security controls are verifiable.

3. The Model

The model consists of one *firm* in charge of protecting a digital asset or service using two security controls, and one *standard maker* aiming to optimize social welfare by setting security standards that the firm must abide by.

3.1 The Firm

Whenever a firm stores information for (or provides services to) their customers and supply-chain stakeholders, there is a possibility that customers or other stakeholders may be affected when this firm's information security is breached. In this model, at the time of the breach, let the damage to the firm be a constant D_F and the damage to social welfare be D_{SW} $D_{SW} > D_F > 0$. Let damages include opportunity costs. We also assume that any contingent transfer payments upon a security incident (e.g. ones designated in a Service-Level Agreement (SLA)) are included in D_F.

Note that the firm's primary business can be (and in practice often is) different from security provision. For example, CardSystems Solutions provides security services yet its primary business function is to process credit card transactions. We focus on security issues in this paper and assume that, notwithstanding a security compromise, the firm earns a business profit of V_F and the society in total receives a benefit of V_{SW}, $V_{SW} > V_F > 0$.

3.2 Security Controls

The firm protects the digital asset using security controls. A common practice is for organizations to deploy multiple security controls (*controls* in short), such as multiple firewalls. In this model we consider a simple case in which, in order to protect the digital asset, the firm needs to invest in two security controls, V and N. Let b_i represent the probability that attackers successfully breach the security control i,

$i \in \{V, N\}$. We consider the following breach probability function:

$$b_i = \begin{cases} \exp\left(-\frac{m_i}{K_i t_i}\right) & \text{if } t_i > 0 \\ 0 & \text{if } t_i = 0 \end{cases}$$

The breach probability of control $i (i \in \{V, N\})$ is a negative exponential function that decreases in the firm's investment, m_i, on control i. Investment can take diverse forms such as technological purchases, development and maintenance, and labor. We assume that all investment can be measured in total by a non-negative monetary variable, m_i. The breach probability increases in the effort by the representative attacker, t_i (or the collective effort of multiple attacker). Hereafter we refer to t_i as "attack intensity" for ease of exposition. The possible difference between constants K_V and K_N captures the heterogeneous cost structures in the two controls: for example, given the same attack intensities and if $K_V < K_N$, were to reach the same level of protection (i.e. $b_V = b_N$) control V requires less investment than control N. Hereafter we say control V is more (less) cost-effective than control N if $K_V < K_N$ ($K_V > K_N$). To rule out the uninteresting case of no firm investment on security controls, we assume $\max\{K_V, K_N\} < D_F$.

For any given positive attack intensity, the negative exponential form of the breach probability function implies that the marginal investment needed to reduce b_i by a unit increases in b_i – in other words, the firm faces a convex security cost function. Furthermore, it ensures that b_i falls into region [0, 1]. This functional form also implies that, for any given positive attack intensity, perfect security (i.e. $b_i = 0$) is unattainable. The negative exponential function has been used by others in modeling security breach probabilities [36]. For notational succinctness, we slightly abuse the notation and treat $\exp\left(-\frac{m_i}{K_i t_i}\right)$ as $\lim_{\tau \to 0}\left(-\frac{m_i}{K_i \tau}\right)$ when $t_i = 0$, and therefore use $b_i = \exp\left(-\frac{m_i}{K_i t_i}\right)$ for any non-negative t_i instead of the conditional form in.

Let function $\omega(b_V, b_N)$ denote the probability that attackers successfully compromise the digital asset or service. We can then write the firm's expected utility as:

$$U_F = V_F - \omega(b_V(m_V, t_V), b_N(m_N, t_N))D_F - m_V - m_N$$

3.3 Three Security Configurations

We describe the relationship between the two controls and the security of the digital asset. We consider three basic and commonly-seen relationships – which we refer to as *security configurations*.

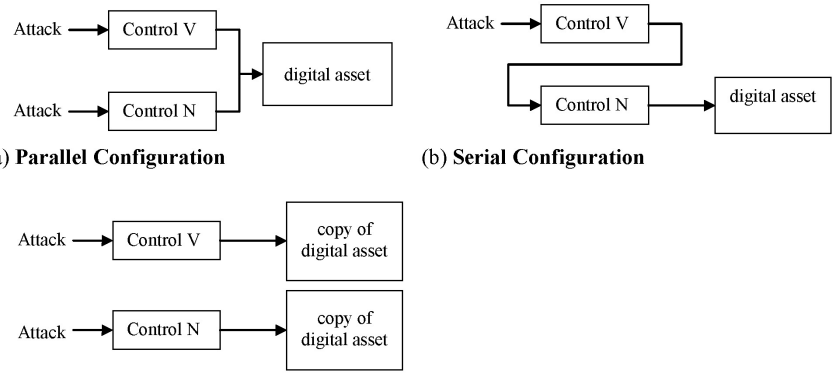
Information security attacks can lead to two broad categories of detrimental consequences for businesses: unauthorized access of information and service disruptions [22]. If a

firm's security concern is on unauthorized access, naturally the firm would like to plug all possible loopholes through which threats may penetrate. Consider a scenario with two such loopholes, where breaching of either one can lead to unauthorized access. The firm can then deploy one security control to each loophole — called the *parallel configuration* — as shown in Figure 1a. In other words, parallel configuration refers to the case where the digital asset is compromised when either control is breached. One commonly seen example of the parallel configuration is a corporate network that is linked to the Internet at multiple access points, whereas each access point is secured by a separate firewall — a widely used type of security control.

Breaching any of such firewalls will then expose internal data to an attacker. Under parallel configuration, $\omega(b_V, b_N) = 1-(1-b_V)(1-b_N) = b_V + b_N - b_V b_N$.

An alternative scenario — the serial configuration — is when the firm has only one security loophole, and the firm deploys two or more controls sequentially to defend against this loophole, as shown in <Figure 1b>. In other words, serial configuration refers to the case where the digital asset is compromised only when both controls are breached sequentially. Under serial configuration, $\omega(b_V, b_N) = b_V b_N$. Moreover, because the first security control in a serial configuration (e.g. V in <Figure 1b>) already filters out some attacks, the second security control (N) faces an often much-reduced attack intensity than the first one.

When a firm's security concern is on service disruption instead of on unauthorized access, a popular defense method is to create redundant and distributed copies of the same data or service, and then to protect every copy. For example, Denial-of-Service (DoS) attacks are a frequent type of disruption attacks to web services [11]. A popular defense for many web service operators, such as CNN.com and MTV.com, is to



(a) **Parallel Configuration** (b) **Serial Configuration**

(c) **Best-shot Configuration** (damage to asset happens only if both copies are compromised)

〈Figure 1〉 Three Security Configurations

deploy their services to multiple web servers so that if one server experiences service outage due to attacks, other redundant servers can takeover and resume the service. Formally, best-shot configurationrefers to the case where digital asset security depends only on the strongest link between the two controls, as illustrated in <Figure 1(c)>. Another example of the best-shot configuration is thepopular practice of using a Disaster Recovery Plan (DRP) to address possible natural or man-made disasters that destroy IT data or infrastructure: unrecoverable data or service loss can be avoided as long as at least one backup is not affected by a disaster. The breach probability function under best-shot configuration has the same form as the one under serial configuration, i.e., $\omega(b_V, b_N) = b_V b_N$. Nevertheless, these two security configurations differ significantly in that, under best-shot configuration, neither control filters out attacks for the other.

Note that in business practice, security configurations can be a complex combination of the aforementioned basic ones. As a first theoretical exploration on understanding the impact of security configurations on standardization in the presence of an unverifiable control, we focus on basic security configurations.

3.4 The Standard maker and Verifiability of Security Controls

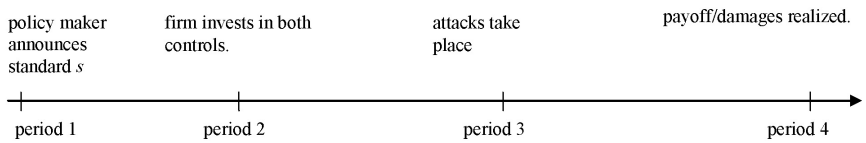
The standard maker's objective is to maximize the expected social welfare, U_{SW} as shown below, via security standardization.

$$U_{SW} = V_{SW} - \omega(b_V(m_V, t_V), b_N(m_N, t_N))D_{SW} - m_V - m_N$$

While the direct control of security investments is in the hands of the firm, the standard maker can indirectly affect firm investments through regulatory standards (such as PCI-DSS) on any verifiable security control. In this paper we are interested in the case where security control V is verifiable to the standard maker while N is not. For example and in the context of reducing firewall breaches, control V can be the frequency of external reviews of firewall rule sets that is contractually verifiable and thus enforceable by the standard maker; control N can be a firm's managerial effort, whereas such effort is hard to monitor and quantify.

As a result, the standard maker can only mandate a standard s for control V. A standard for control V is an investment threshold that the firm must match or exceed. For the scope of this paper, we focus on security standards that have strict enforcement power, so that the affected firm has to unconditionally confirm it. Two widely applicable examples are NIST security standards and PCI-DSS: NIST standards are mandatory for all affected US governmental agencies [18]; PCI-DSS is mandatory for all merchants that "accepts, transmits or stores any (credit or debit) cardholder data."

<Figure 2> shows the timing of the model.



〈Figure 2〉 Timing of the Model

The standard maker first announces the standard, s, for control V. The firm then chooses its investments m_V and m_N on the security controls. Possible security attacks then take place.

4. Standardization

In this section we study how the existence of the unverifiable security control N affects firm investments and the optimal security standard on the verifiable security control V. Furthermore, we compare it with two benchmark standards with which the standard maker uses for practical use.

As the attacks are automated, both t_V and t_N are exogenously given under either parallel configuration or best-shot configuration, which we consider as constants. Without loss of generality, we normalize both t_V and t_N to constant one under these two security configurations. Under serial configuration, let the attack intensity to the first security control be one, whereas the attack intensity to the second control will be lower and will depend on the effectiveness of the first control in blocking attacks.

Next we analyze security standardization and firm response for each of the three security configurations after understanding two benchmark standards.

4.1 Bounded-Rational Standard

4.1.1 Naïve Standard

The first case – the naive standard – is when the policy maker is naive in the sense that it is not aware of the existence of the unverifiable control N. In other words, the naive policy maker incorrectly believes that $\omega(b_V) = 1 - b_V$. This can be the case, for example, if the policy maker simply ignores all security controls that it cannot monitor and regulate. Alternatively, the naive-information benchmark may arise even for a policy maker that pays due diligence if a new type of security control is invented after the policy maker has already published the standard. Intuitively, not aware of the unverifiable control, the naive policy maker over-estimates the marginal impact of the verifiable control on overall firm security.

4.1.2 Complete Information Standard

The second benchmark case – *the complete-information standard* – is when the poli-

cy maker can set verifiable standards over both controls V and N. Under serial configuration first best policy maker's choice depends critically on the relative cost-efficiency of the security controls. When the verifiable control V is more cost-efficient (in that $K_V \le K_N$), the first best policy maker should put high standard on control V (thus the term "best-shot"). The firm will find that control V will always have a lower marginal cost of defense than control N at any security level if $K_V \le K_N$. Therefore, it is not worthwhile to invest in the unverifiable control N.

4.2 Parallel Configuration

Throughout this subsection, subscript "PC" means "parallel configuration."

$\omega(b_V,\ b_N) = b_V + b_N - b_V b_N = \exp\left(-\frac{m_V}{K_V}\right) + \exp\left(-\frac{m_N}{K_N}\right) - \exp\left(-\frac{m_V}{K_V} - \frac{m_N}{K_N}\right)$ under parallel configuration. In period 2 and given any arbitrary standard S_{PC} for control V that is imposed by the standard maker, the firm's optimization problem is:

$$\max_{m_V,\ m_N} U_F = V_F - \left(\exp\left(-\frac{m_V}{K_V}\right) + \exp\left(-\frac{m_N}{K_N}\right) - \exp\left(-\frac{m_V}{K_V} - \frac{m_N}{K_N}\right)\right)$$
$$D_F - m_V - m_N,\ \text{s.t.},\ m_V \ge s_{PC}$$

For notational convenience, denote $\tilde{b}_V \equiv \frac{(D_F + K_V - K_N - \sqrt{(D_F + K_V - K_N)^2 - 4K_N D_F})}{2D_F}$ and $\tilde{b}_N \equiv \frac{(D_F - K_V + K_N - \sqrt{(D_F - K_V + K_N)^2 - 4K_N D_F}}{2D_F}$.

$\tilde{b}_V(\tilde{b}_N)$ is the firm's optimal choice of breach probability on control V (N) under parallel configuration when there is no security standard. The next lemma presents the firm's optimal investments.

Lemma 1: *Under parallel configuration and given standard s_{PC} for control V*:

i. *If* $s_{PC} < K_V ln(1/\tilde{b}_V)$, $m_V^* = K_V ln(1/\tilde{b}_V)$ *and* $m_N^* = K_N ln(1/\tilde{b}_N)$

ii. If $s_{PC} \ge K_V ln(1/\tilde{b}_V)$, $m_V^* = s_{PC}$ and $m_N^* = K_N ln\left(\frac{D_F(1-\exp(-s_{PC}/K_V))}{K_N}\right)$

Proofs are in the Appendix. Lemma 1 shows that, for the security standard S_{PC} to have impact on firm investments, it has to be high enough (i.e. more than $K_V ln(1/\tilde{b}_V)$). Given $s_{PC} \ge K_V ln(1/\tilde{b}_V)$, a higher standard not only directly forces the firm to invest more in the verifiable control, it also indirectly incentivizes the firm to invest more on the unverifiable control. We capture this important observation in the following proposition.

Proposition 1: *Under parallel configuration, the firm's investment on the unverifiable security control increases in the standard on the verifiable control when the standard is high enough* ($s_{PC} \ge K_V ln(1/\tilde{b}_V)$).

When a higher standard directly forces the firm to invest more heavily on the verifiable control, Proposition 1 shows that the firm finds the marginal return from investing on the unverifiable control increases accordingly – thus it invests more on the unverifiable control [20].

We next analyze optimal standard decision by the standard maker in period 1. Analytically, because results under $s_{PC} < K_V ln(1/\tilde{b}_V)$ are equivalent to the one under $s_{PC} = K_V ln(1/\tilde{b}_V)$, it is sufficient for us to only consider $s_{PC} \geq K_V ln(1/\tilde{b}_V)$. The standard maker's optimization problem is

$$\max_{s_{PC}} U_{SW} = V_{SW} - \left(\exp\left(-\frac{m_V}{K_V}\right) + \exp\left(-\frac{m_N}{K_N}\right) - \exp\left(-\frac{m_V}{K_V} - \frac{m_N}{K_N}\right)\right) D_{SW} - m_V - m_N, \quad \text{where } s_{PC} \geq K_V ln(1/\tilde{b}_V), \quad m_V = s_{PC} \text{ and } m_N = K_N ln\left(\frac{D_F(1-\exp(-s_{PC}/K_V))}{K_N}\right).$$

It turns out the standard maker will always choose a standard high enough so that the firm is forced to invest more on both controls (than it would under no standard):

Lemma 2: *Under parallel configuration, the socially optimal standard on control V is* $s^*_{PC} = K_V \ln\left(\frac{1}{b^*_{PC}}\right)$, where $b^*_{PC} = \frac{(D_{SW} + K_V - K_N - \sqrt{(D_{SW} + K_V - K_N^2) - 4K_N D_{SW}})}{2D_{SW}}$.

It is now worthwhile for us to compare the results in Lemma 2 to the ones under a *complete-information benchmark*. Consider, for a moment, the scenario where the standard maker can impose and enforce standards on both security controls – we call this scenario the complete-information benchmark, and the standard maker's optimal standards under this benchmark *complete-information standards*. In other words, complete-information standards are the optimal standards when both security controls are verifiable. From equation and $\omega(b_V, b_N) = b_V + b_N - b_V b_N$ it is straightforward to verify that the complete-information standard on control V is exactly s_{PC}. Therefore:

Proposition 2: *Under parallel configuration, the standard maker should simply impose the complete-information standard for security control V.*

Proposition 2 implies that, even though the standard maker is facing a complex situation where not all security controls are verifiable, its optimal choice of standard is nevertheless simple under parallel configuration: the standard maker can simply design socially-optimal standards as if all controls are verifiable, and then impose it wherever feasible.

There are, nevertheless, two caveats to this result on adopting a complete-information standard. First, though the firm's investment on the unverifiable control N is indirectly pushed up because of the high complete-information standard on control V, this investment is still lower than the socially-optimal level. As a re-

sult, social-optimality (as in the complete information benchmark) is not attainable. Second and as we will see shortly, this simple policy of standardization applies only to the parallel configuration, as optimal standards under the other two security configurations are sharply different.

4.3 Best-Shot Configuration

Similar to the last sub-section, we use backward induction to analyze best-shot configuration. Throughout this subsection, subscript "BC" means "best-shot configuration." Under best-shot configuration, $\omega(b_V, b_N) = b_V b_N = exp\left(-\frac{m_V}{K_V} - \frac{m_N}{K_N}\right)$. For any given standard s_{BC} imposed on control V, the firm's optimization problem in period 2 is:

$$\max_{m_V, m_N} U_F = V_F - \left(exp\left(-\frac{m_V}{K_V} - \frac{m_N}{K_N}\right)\right),$$
$$D_F - m_V - m_N \quad \text{s.t.,} \quad m_V \geq s_{BC}.$$

Lemma 3: *Under best-shot configuration and given standard s_{BC} on security control V:*

i. If $K_V \leq K_N$,
$m_V^* = max\{K_V ln(D_F/K_V), s_{BC}\}$ *and* $m_N^* = 0$.

ii. If $K_V > K_N$ and $s_{BC} \geq K_V \ln(D_F/K_N)$,
$m_V^* = s_{BC}$ *and* $m_N^* = 0$.

iii. If $K_V > K_N$ and
$s_{BC} < K_V \ln(D_F/K_N)$, $m_V^* = s_{BC}$ *and*
$$m_N^* = K_N \ln\left(\frac{\exp(-s_{BC}/K_V) D_F}{K_N}\right).$$

Unlike parallel configuration, under best-shot configuration firm's investments depend critically on the relative cost-efficiency of the security controls. When the verifiable control V is more cost-efficient (in that $K_V \leq K_N$), the firm should give up the unverifiable control N and focus its investment on control V (thus the term "best-shot"). Intuitively, though the marginal cost of defense increases in the security level of any security control, the multiplicative form of the breach probability function ($\omega(b_V, b_N) = b_V b_N$) implies that the firm will find that control V will always have a lower marginal cost of defense than control N at any security level if $K_V \leq K_N$. Therefore, it is not worthwhile to invest in the unverifiable control N.

The story is slightly more complicated when the unverifiable control N is more cost-efficient (i.e. $K_V > K_N$). In this case, the firm is forced to invest in the non-efficient control V. Lemma 3 (iii) shows that, if the standard is not high, the firm will abide by the standard, yet will also invest in control N to take advantage of its cost-efficiency. If the standard is very high, as shown in Lemma 3 (ii), the firm is forced to invest heavily on control V to the point where it does not see any benefit from additional investment on control N even if the latter is more cost-efficient. It is obvious that, from the firm's perspective, a standard on the verifiable control leads to inefficient investment when the other

control is more cost-efficient. The next proposition describes the impact of the standard on the unverifiable control.

Proposition 3: *Under parallel configuration, the firm's investment on the unverifiable security control*

i. decreases in the standard on the verifiable control if the verifiable control is less cost-efficient and the standard is low enough (i.e. $s_{BC} < K_V ln(D_F / K_N)$*);*

ii. is zero otherwise.

We next describe the standard maker's optimal decision in period 1. For ease of exposition, define $f(r) \equiv -r + rlnr + rln\left(\frac{K_N}{D_{SW}}\right) + \frac{D_{SW}}{D_F} - \ln(K_N / D_F)$ and let $\hat{r}$ be the solution to $f(\hat{r}) = 0$.

Lemma 4: $s^*_{BC} = 0$ *if* $\frac{K_V}{K_N} \geq \max\{\hat{r}, 1\}$, $s^*_{BC} = K_V ln(D_{SW} / K_V)$ *otherwise.*

To understand the intuitions behind Lemma 4, we now introduce a second benchmark scenario – *the naive-information benchmark*, which refers to the scenario where the standard maker is unaware of the existence of the unverifiable control. In other words, the standard maker naively (and incorrectly) believes that $\omega(b_V, b_N) = b_V$. This can be the case, for example, if the standard maker simply ignores all security controls that it cannot monitor and regulate. Alternatively, the naive-information benchmark may arise even for a standard maker that pays due diligence if a new type of security control is invented after the standard maker has already published the standard. From and $\omega(b_V, b_N) = b_V$, we know the optimal standard under the naive-information benchmark is $K_V ln(D_{SW} / K_V)$, which we refer to as the *naive-information standard.*

Proposition 4: *Under best-shot configuration, the standard maker should either impose the naive-information standard (if* $\frac{K_V}{K_N} < max\{\hat{r}, 1\}$*) or not impose any standard. The firm will accordingly invest on only one security control.*

The standard maker's decision problem is more complicated under best-shot configuration (as compared to parallel configuration) because it now has to judge when to impose a standard. When the verifiable control is more cost-efficient (i.e. $K_V < K_N$), a high standard induces the firm to make socially-optimal investment. Furthermore and interestingly, the standard maker may force the firm to invest in the verifiable control even *if* it is less cost-efficient as compared to the unverifiable control, as in the case $max\{\hat{r}, 1\}K_N > K_V > K_N$. Intuitively, in this case the standard maker is trading-off two effects: on the one hand, forcing the firm to invest heavily in the less cost-effi-

cient control hurts firm profit; on the other hand, a high standard benefits consumer surplus – as lacking a standard the firm will not invest as high even in the cost-efficient control. When the efficiency loss is not too high (i.e. K_V is upper-bounded by $max\{\hat{r}, 1\}K_N$), the second effect dominates the first one from the standard maker's perspective.

Once the question of when to impose a standard is answered, the standard itself is remarkably simple: it is the naive-information standard. This finding under best-shot configuration contrasts sharply with the finding regarding the optimality of the complete-information standard under the parallel configuration.

Under best-shot configuration and given optimal standards, the firm will always put all investment into the "best-shot" security control. This result is consistent with prior theoretical findings such as Varian [33]. This is a unique characteristic of this security configuration as in all other security configurations, such as the serial configuration which we next discuss, we will see the firm investing in and balancing both security controls.

4.4 Serial Configuration

Serial and best-shot configurations are similar in that they have the same breach probability function: $\omega(b_V, b_N) = b_V b_N = exp\left(-\frac{m_V}{K_V} - \frac{m_N}{K_N}\right)$. In other words, to compromise the digital asset and cause damage, in both security configurations attackers have to breach both security controls. That said, a key difference between these two security configurations is that, under serial configuration, the first security control (e.g. V in <Figure 1b>) filters and blocks some attacks before traffic arrives at the second control (N in <Figure 1b>). As a result, one should expect a lower attack intensity – conditional on how secure the first control is – toward the second control in serial configuration.

Therefore, unlike in previous sub-sections where we normalize both attack intensities t_V and t_N to constant one, in this subsection only the first security control has a normalized attack intensity of one. In this paper we further restrict our attention to the case where the first security control is verifiable (as in <Figure 1b>). Thus $t_V = 1$. t_N is assumed as follows:

$$t_N = \alpha b_V$$

Where α is a constant in (0, 1]. The above linear equation is the simplest formula to capture the idea that, the better protection the first security control offers (thus a lower breach probability, b_V), the less likely attacks can sneak through this first control and arrive at the second control. can be rewritten as $t_N = t_N(m_V) = \alpha\, exp(-m_V/K_V)$.

For any given standard s_{SC} imposed on control V, the firm's optimization problem in

period 2 is: $\max_{m_V, m_N} U_F = V_F - \left(exp\left(-\frac{m_V}{K_V} - \frac{m_N}{K_N t_N(m_V)} \right) \right) D_F - m_V - m_N$, s.t., $m_V \geq s_{BC}$.

Lemma 5: *Under serial configuration and given standard s_{SC} on security control V:*

i. If $s_{SC} \geq K_V \ln\left(\frac{K_N \alpha \left(1 + \ln\left(\frac{D_F}{K_N \alpha} \right) \right)}{K_V} \right)$,

$m_V^* = s_{SC}$ *and*

$m_N^* = K_N \alpha \exp(-s_{SC}/K_V) \ln\left(\frac{D_F}{K_N \alpha} \right)$

ii. Otherwise,

$m_V^* = K_V \ln\left(\frac{K_N \alpha \left(1 + \ln\left(\frac{D_F}{(K_N \alpha} \right) \right)}{K_V} \right)$ *and*

$m_N^* = K_V \left(1 - \frac{1}{1 + \ln\left(\frac{D_F}{K_N \alpha} \right)} \right)$

Proposition 5: *Under serial configuration, the firm's investment on the unverifiable security control decreases in the standard on the verifiable control when the standard is high enough* (*i.e. when* $s_{SC} \geq K_V \ln\left(\frac{K_N \alpha \left(1 + \ln\left(\frac{D_F}{K_N \alpha} \right) \right)}{K_V} \right)$).

Under serial configuration, a high standard on the verifiable control results in a low probability of any attack passing through this control [20]. As a result, t_N will be significantly lower than t_V (which is normalized to 1), which reduces the need to have strong security on the unverifiable control, as shown in Proposition 5.

That said, this reduction in the investment on control N is not as extreme as the one in the best-shot configuration: in the latter there is no investment at all on control N when the standard is high enough; while in the former investment on N is always positive. This is because a reduction in attack intensity t_N improves the marginal benefit of each unit of investment on control N because breach probability $b_N$is an increasing function of t_N. This improvement turns out to be significant enough: even if the verifiable control is ex ante more cost-efficient (i.e. $K_V < K_N$), from Lemma 5 (i) it is straightforward to verify that $K_N t_N(m_V) < K_V$ always holds. Therefore, ex post and due to the reduction in attack intensity on control N, investment on this control becomes cost-efficient. Next we describe the standard maker's optimal decision in period 1 that maximizes social welfare.

Proposition 6: *Under serial configuration, the standard maker should impose a standard of* $s_{SC}^* = max\left\{ K_V ln\left(\frac{K_N \alpha}{K_V} \left(\frac{D_{SW}}{D_F} + ln \frac{D_F}{K_N \alpha} \right) \right),\ 0 \right\}$.

5. Concluding Remarks

This paper is a first study, from a standard maker's perspective, on whether and how the existence of an unverifiable security control af-

fects an optimal security standard on another related and verifiable security control. We find that, except for some cases under the best-shot configuration, the unverifiable control will affect the optimal standard on the verifiable control. We further show that the specific security configuration – namely, how the two controls together protect a firm's digital asset – plays a critical role in deciding the optimal standard. Parallel configuration calls for a high standard, serial configuration calls for a low standard, and under best-shot configuration the unverifiable control has no impact on the standard if this control is less cost-efficient than the verifiable control.

It is not optimal, on the one hand, for the standard maker to ignore the existence of any unverifiable security control – named naïve standard maker in this paper – when designing security standards. The only exception is when, under best-shot configuration, the verifiable control is more cost-efficient than the unverifiable control. The naïve standard maker is more likely to overshoot its standard, brining less social welfare to security ecosystem. On the other hand, it is only optimal to consider every control as verifiable – named complete-information standard maker – for parallel configuration. That is, different to the intuition, complete-information standard does not necessarily bring higher social welfare. Therefore, the standard maker should set or benchmark different security standards under different security configurations.

This paper differs from Lee et al. [20] in many aspects. First, Lee et al. [20] mainly focuses on how the unverifiable control affects organizational security, but this paper places emphasis on rational and bounded-rational policy makers. Second, best-shot configuration is considered since it is the popular practice in a Disaster Recovery Plan (DRP) in which unrecoverable data or service loss can be avoided as long as at least one backup is not affected by a disaster. More interestingly, it provides an exception in which naïve standard does not necessarily offer less social welfare than complete-information standard and identical to optimal standard. Last, this paper incorporates more popular economic model, Varian [33] work, making the standard maker's decision mathematically traceable.

This research on the relationship between security control verifiability and security standard can be extended in a number of ways. First, in practice security configurations can be more complicated than the three basic forms discussed in this paper, and can involve more than two controls. The question of whether a complicated security configuration can always be decomposed into the three basic forms is intriguing. Second, subject to data availability, our research offers a number of empirically testable results, such as the ones on how security configuration affects a firm's investment on unverifiable controls. A follow-up empirical study will be valuable, as far as our knowledge is concerned there are few research efforts that

approach empirically the study of how security standards affect firm investment on security controls and attacker strategy.

References

[1] Adams, A. and Sasse, M. A., "Users are Not the Enemy," Communications of the ACM, Vol. 42, No. 12, pp. 41-46, 1999.

[2] Battigalli, P. and Maggi, G., "Rigidity, Discretion, and the Costs of Writing Contracts," The American Economic Review, Vol. 92, No. 4, pp. 798-817, 2002.

[3] Bernheim B. D. and Whinston, M. D., "Incomplete Contracts and Strategic Ambiguity," The American Economic Review, Vol. 88, No. 4, pp. 902-932, 1998.

[4] Cavusoglu, H., Mishra, B., and Raghunathan, S., "The Value of Intrusion Detection Systems in Information Technology Security Architecture," Information Systems Research, Vol. 16, No. 1, pp. 28-46, 2005.

[5] Cavusoglu, H., Raghunathan, S., and Cavusoglu, H., "Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems," Information Systems Research, Vol. 20, No. 2, pp. 198-217, 2009.

[6] Crawford, V., "Lying for Strategic Advantage: Rational and Boundedly Rational Misrepresentation of Intentions," The American Economic Review, Vol. 93, No. 1, pp. 133-149, 2003.

[7] Culnan, M. J. and Williams, C. C., "How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches," MIS Quarterly, Vol. 33, No. 4, pp. 673-687, 2009.

[8] Dey, D., Fan, M., and Zhang, C., "Design and Analysis of Contracts for Software Outsourcing," Information Systems Research, Vol. 21, No. 1, pp. 93-114, 2010.

[9] Dye, R. A., "Auditing Standards, Legal Liability, and Auditor Wealth," The Journal of Political Economy, Vol. 101, No. 5, pp. 887-914, 1993.

[10] Ewert, R. and Wagenhofer, A., "Economic Effects of Tightening Accounting Standards to Restrict Earnings Management," The Accounting Review, Vol. 80, pp. 1101-1024, 2005.

[11] Geng, X., Huang, Y., and Whinston, A. B., "Defending Wireless Infrastructure Against the Challenge of DDoS Attacks," ACM Journal on Mobile Networking and Applications, Vol. 7, No. 3, pp. 213-223, 2002.

[12] Gordon, L. A., Loeb, M., and Lucyshyn, W., "Sharing Information on Computer Systems Security: An Economic Analysis," Journal of Accounting Public Policy, Vol. 22, No. 6, pp. 461-485, 2003.

[13] Grossklags, J., Christin, N., and Chuang, J., "Secure or Insure? A Game-Theoretic Analysis of Information Security Games," Proceedings of the 17th International

World Wide Web Conference, 2008.

[14] Hausken, K., “Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability,” Information Systems Frontiers, Vol. 8, No. 5, pp. 338-349, 2006.

[15] Hausken, K., “Information sharing among firms and cyber attacks,” Journal Accounting Public Policy, Vol. 26, No. 6, pp. 639-688, 2007.

[16] Hendricks, K. and McAfee, R. P., “Feints,” Journal of Economics & Management Strategy, Vol. 15, No. 2, pp. 431-456, 2006.

[17] Hui, K. L., Hui, W., and Yue, W. T., “Information Security Outsourcing with System Interdependency and Mandatory Security Requirement,” Journal of Management Information Systems, Vol. 29, No. 3, pp. 117-155, 2012.

[17] Keblawi, F. and Sullivan, D., “The Case for Flexible NIST Security Standards,” IEEE Computer Society, June, pp. 19-26, 2007.

[18] Krebs, R., Hackers Test Limits of Credit Card Security Standards, Washington Post, April 16, 2009, available at voices.washingtonpost.com/securityfix/2009/04/the_number_scale_and_sophistic.html.

[19] Lee, C. Geng, X., and Raghunathan, S., “Mandatory Standards and Organizational Information Security,” Information Systems Research, Vol. 27, No. 1, pp. 70-86, 2016.

[20] Lee, C., Geng, X., and Raghunathan, S., “Contracting Information Security in the Presence of Double Moral Hazard,” Information Systems Research, Vol. 24, No. 2, pp. 295-311, 2013.

[21] Loch, K., Carr, H., and Warkentin, M., “Threats to Information Systems: Today’s Reality, Yesterday’s Understanding,” MIS Quarterly, Vol. 16, No. 2, pp. 173-186, 1992.

[22] Miller, A. R. and Tucker, C. E., “Encryption and Data Loss, The Ninth Workshop on the Economics of Information Security,” Harvard University, USA, p. 29, 2010.

[23] Morse, E. A. and Raval, V., “PCI DSS: Payment card industry data security standards in context,” Computer Law& Security Report, Vol. 24, pp. 540-554, 2008.

[24] Narasimhan, H., Varadarajan, V., and Rangan, C. P., “Towards a Cooperative Defense Model Against Network Security Attacks,” Tenth Workshop on the Economics of Information Security, 2010.

[25] Romanosk, S., Telang, R., and Acquisti, A., “Do Data Breach Disclosure Laws Reduce Identity Theft?,” Seventh Workshop on the Economics of Information Security, June 25-28, 2008.

[26] Ross, R., “Managing Enterprise Security Risk with NIST Standards,” IEEE Computer Society, August, pp. 88-91, 2007.

[27] Rothke, B. and Mundhenk, D., Sue the Auditor and Shut Down the Firm (July 9), 2009, Available at http://www.csoonline.com/article/496923/Sue_the_Auditor_and_Shut_

Down_the_Firm.

[28] Schechter, S. E. and Smith, M. D., “How Much Security is Enough to Stop a Thief?,” Lecture Notes in Computer Science, Vol. 2742, pp. 122-137, 2003.

[29] Schwartz, R., “Legal Regimes, Audit Quality and Investment,” The Accounting Review, Vol. 72, No. 3, pp. 385-406, 1997.

[30] Shim, W., “An Ex Ante Evaluation Method for Assessing a Government Enforced Security Measure,” The Journal of Society for e-Business Studies, Vol. 20, No. 4, pp. 241-256, 2015.

[31] Tirole, J., “Cognition and Incomplete Contracts,” The American Economic Review, Vol. 99, No. 1, pp. 265-294, 2009.

[32] Varian, H., “System Reliability and Free Riding,” Economics of Information Security, Kluwer, pp 1-15, 2004.

[33] Willekens, M., Steele, A., and Miltz, D., “Audit Standards and Auditor Liability: A Theoretical Model,” Accounting and Business Research, Vol. 26, No. 3, pp. 249-264, 1996.

[34] Zetter, K., In Legal First, Data-Breach Suit Targets Auditor, Wired (June 2), 2009, Available at http://www.wired.com/threatlevel/2009/06/auditor_sued/.

[35] Zhao, X, Xue, L., and Whinston, A. B., “Managing Interdependent Information Security Risks: A Study of Cyberinsurance, Managed Security Service and Risk Pooling,” International Conference on Information Systems, Phoenix, AZ, 2009.

〈Appendix〉 Given Page limit, we Only Provide Proofs for kEy Steps

Proof of Lemma 1 (parallel configuration):

The firm's decision problem can be solved by Kuhn-Tucker condition.

$$\max_{b_V,\, b_N} L_{PC} = V_F - \left(\exp\left(-\frac{m_V}{K_V}\right) + \exp\left(-\frac{m_N}{K_N}\right) - \exp\left(-\frac{m_V}{K_V} - \frac{m_N}{K_N}\right)\right) D_F - m_V - m_N + \lambda_{PC}(m_V - s_{PC})$$

$$\frac{\partial L_{PC}}{\partial m_V} = \left(\frac{1}{K_V}\exp\left(-\frac{m_V}{K_V}\right) - \frac{1}{K_V}\exp\left(-\frac{m_V}{K_V} - \frac{m_N}{K_N}\right)\right) D_F - 1 + \lambda_{PC} = 0$$

$$\frac{\partial L_{PC}}{\partial m_N} = \left(\frac{1}{K_N}\exp\left(-\frac{m_N}{K_N}\right) - \frac{1}{K_N}\exp\left(-\frac{m_V}{K_V} - \frac{m_N}{K_N}\right)\right) D_F - 1 = 0$$

For any inner solution, λ_{PC} must have a zero value, i.e. $m_V > s_{PC}$. The solutions to the above two equations are $m_V^* = -K_V ln(b_V)$ and $m_N^* = -K_N ln(b_N)$. When the standard, s_{PC}, is greater than m_V, however, two equations have a corner solution, i.e., $m_V = s_{PC}$. Therefore, the solutions of two equations are $m_V^* = s_{PC}$ and $\mathrm{m}_\mathrm{N}^* = -K_N ln \dfrac{K_N}{D_F(1-\exp(-s_{PC}/K_V))}$. Q.E.D.

Proof of Lemma 2:

$$\begin{aligned} \mathrm{U_{SW}} &= V_{SW} - (b_V + b_N - b_V b_N) D_{SW} - m_V - m_N \\ &= V_{SW} - \left(b_{PC} + \frac{K_N}{D_F}\right) D_{SW} + K_V ln\, b_{PC} + K_N ln \frac{K_N}{D_F(1-b_{PC})} \end{aligned}$$

From $\dfrac{\partial \mathrm{U_{SW}}}{\partial \mathrm{b_{PC}}} = -D_{SW} + \dfrac{K_V}{b_{PC}} + \dfrac{K_N}{(1-b_{PC})} = 0$ we have

$$b_{PC}^* = \frac{D_{SW} + K_V - K_N - \sqrt{(D_{SW} + K_V - K_N)^2 - 4D_{SW}}K_V}{2D_{SW}}.$$

We can transform $\mathrm{b_{PC}^*}$ into the following:

$$\mathrm{b_{PC}^*} = \frac{2K_V}{\left(D_{SW} + K_V - K_N + \sqrt{(D_{SW} + K_V - K_N)^2 - 4D_{SW}K_V}\right)}.$$

$\dfrac{\partial \mathrm{b_{PC}^*}}{\partial \mathrm{D_{SW}}} = \sqrt{(D_{SW} + K_V - K_N)^2 - 4D_{SW}K_V} + [(D_{SW} + K_V - K_N)]$. If $D_{SW} > K_V + K_N$, $\mathrm{b_{PC}^*}$ is a decreasing function of $\mathrm{D_{SW}}$. Therefore, $\mathrm{b_{PC}^*} < \tilde{b}_V$ which means $\mathrm{s_{PC}^*}$ is always larger than $-K_V ln\, b_V$. Q.E.D.

Proof of Lemma 5 (serial configuration):

$$\max_{b_V,\, b_N} L_{SC} = V_F - \left(\exp\left(-\frac{m_V}{K_V T} - \frac{m_N}{K_N t_N}\right)\right) D_F - m_V - m_N + \lambda_{SC}(m_V - s_{SC})$$

$$\frac{\partial L_{SC}}{\partial m_V} = \left(\exp\left(-\frac{m_V}{K_V T} - \frac{m_N}{K_N t_N}\right)\left(\frac{1}{K_V T} - \frac{m_N t_N(m_V)}{K_N t_N^2(m_V)}\right)\right) D_F - 1 + \lambda_{SC} = 0$$

$$\frac{\partial\, L_{SC}}{\partial\, m_N} = \left(\exp\left(-\frac{m_V}{K_V T} - \frac{m_N}{K_N t_N}\right)\frac{1}{K_N t_N(m_V)}\right) D_F - 1 = 0$$

$$\lambda_{SC}(m_V - s) = 0$$

Given $t_N = \alpha \exp\left(-\frac{m_V}{K_V T}\right)$, we can rewrite $\frac{\partial L_{SC}}{\partial m_V}$ as $\frac{\partial L_{SC}}{\partial m_V} = \left(\exp\left(-\frac{m_V}{K_V T} - \frac{m_N}{K_N t_N}\right)\frac{1}{K_V T}\left(1 + \frac{m_N}{K_N t_N(m_V)}\right)\right) D_F - 1 + \lambda_{SC} = 0$. From $\frac{\partial L_{SC}}{\partial m_N}$ and changed $\frac{\partial L_{SC}}{\partial m_V}$, we have $K_N t_N(m_V) = \frac{(1-\lambda) K_V T}{1 + m/(K_N t_N(m_V))}$. For inner solutions (i.e. $m_V > s$), we need $m_V = 0$.

We already have $m_N = K_V T - K_N \alpha \exp\left(-\frac{m_V}{K_V T}\right)$. From them, we have $K_N \alpha \exp\left(-\frac{m_V}{K_V T}\right) = \frac{k_V T}{1 + \ln(D_F / K_N \alpha)}$.

Therefore, $b_N^* = \frac{K_V T}{K_N \alpha (D_F / K_N \alpha)}$, $m_V^* = K_V T\, ln \frac{(K_N \alpha (1 + \ln(D_F / K_N \alpha)))}{K_V T}$, and $m_N^* = K_V T \ln\left(1 - \frac{1}{1 + \ln(D_F / K_N \alpha)}\right)$

Next we check whether this is indeed an inner solution.

$$m_V^* > s_{SC} \leftrightarrow K_V T\, ln \frac{(K_N \alpha (1 + \ln(D_F / K_N \alpha)))}{K_V T} > s_{SC}.$$

Therefore, if standard is low, we have the inner solution. Otherwise, given $s_{SC} > K_V T \ln \frac{(K_N \alpha (1 + \ln(D_F / K_N \alpha)))}{K_V T}$, we have $m_V^* = s_{SC}$. Now we have $m_N^* = K_N \alpha \exp\left(-\frac{s_{SC}}{K_V T}\right) \ln\left(\frac{D_F}{K_N \alpha}\right)$.

Based on the results above, we know the optimal m_V is decreasing in s_{SC}. To calculate optimal s_{SC}, we only need to consider the case where $s_{SC} > K_V T\, ln \frac{(K_N \alpha (1 + \ln(D_F / K_N \alpha)))}{K_V T}$.

Given $b_V = \exp\left(-\frac{s_{SC}}{K_V T}\right)$ and $b_N = \exp\left(-\frac{m_N}{K_N \alpha \exp(-s_{SC} / K_V T)}\right) = \exp\left(-ln \frac{D_F}{K_N \alpha}\right) = \frac{K_N \alpha}{D_F}$.

$$U_{SW} = V_{SW} - \left(\frac{K_N\alpha}{D_F}\exp\left(-\frac{s_{SC}}{K_V T}\right)\right)D_{SW} - s_{SC} - K_N\alpha \ln\left(\frac{D_F}{K_N\alpha}\right)\exp\left(-\frac{s_{SC}}{K_V T}\right)$$

$$= V_{SW} - s_{SC} - \exp\left(-\frac{s_{SC}}{K_V T}\right)K_N\alpha\left[\frac{D_{SW}}{D_F} + \ln\left(\frac{D_F}{K_N\alpha}\right)\right]$$

$$\frac{\partial U_{SW}}{\partial s_{SC}} = -1 + \exp\left(-\frac{s_{SC}}{K_V T}\right)\left(\frac{K_N\alpha}{K_V T}\right)\left[\frac{D_{SW}}{D_F} + \ln\left(\frac{D_F}{K_N\alpha}\right)\right].$$

If solution is inner, $s^*_{SC} = K_V T \ln\left[\left(\frac{K_N\alpha}{K_V T}\right)\left(\frac{D_{SW}}{D_F} + \ln\left(\frac{D_F}{K_N\alpha}\right)\right)\right]$.

Condition for inner solution: $K_V T ln\left[\left(\frac{K_N\alpha}{K_V T}\right)\left(\frac{D_{SW}}{D_F} + \ln\left(\frac{D_F}{K_N\alpha}\right)\right)\right]$

$$\geq K_V T ln\left[\frac{K_N\alpha(1 + ln D_F/(K_N\alpha))}{K_V T}\right],$$

which is always true. Therefore, $s^*_{SC} = \max\left\{0,\ K_V T ln\left[\left(\frac{K_N\alpha}{K_V T}\right)\left(\frac{D_{SW}}{D_F} + \ln\left(\frac{D_F}{K_N\alpha}\right)\right)\right]\right\}$. Q.E.D.

저 자 소 개

이철호	(E-mail: irontigerlee@kaist.ac.kr)
2000년	부산대학교 경영학부 (학사)
2002년	부산대학교 경영학부 (석사)
2012년	텍사스 주립대학교 댈러스 캠퍼스 경영과학 (박사)
2012~2013년	미국 제이비어 대학교 방문조교수
2013~2016년	중국 하얼빈 공업대학교 경영공학과 부교수
2016년~현재	카이스트 기술경영학부 조교수
관심분야	정보보안경제, 경영분석