The Impact of Professional Information Security Ratings on Vendor Competition[1]

September 2009

Zach Z. Zhou
Center for Digital Strategies
The Tuck School of Business
Dartmouth College
zach.zhou@tuck.dartmouth.edu

M. Eric Johnson
Center for Digital Strategies
The Tuck School of Business
Dartmouth College
m.eric.johnson@tuck.dartmouth.edu

Abstract

Security breaches often stem from business partner failures within the value chain. There have been several recent efforts to develop a common reference for rating the information risk posed by partners. We develop a simple analytical model to examine the impact of such information security ratings on service providers, customers, and social welfare. While some might believe that professional information security ratings would benefit high-security providers and hurt those with lower security, we show that this is not always the case. We find that such ratings can hurt both types of providers or benefit both, depending on the market conditions. Surprisingly, we also find that professional information security ratings do not always benefit the most demanding customers who desire highly secure business partners. Yet, in all cases, we find that social welfare is improved when professional information security ratings are adopted. This result suggests that professional information security ratings should be encouraged through public policy initiatives.

Key words: Economics of Information Security, Information Security Rating, IT Policy and Management, Information Systems

[1] This research was supported by the Institute for Information Infrastructure Protection (I3P) under award 60NANB6D6130 from the U.S. Department of Commerce and the Institute for Security Technology Studies at Dartmouth College under award Number 2006-CS-001-000001 from the U.S. Department of Homeland Security (NCSD). The statements, findings, conclusions, and recommendations are those of the authors and do not necessarily reflect the views of the National Institute of Standards and Technology (NIST), Department of Homeland Security, the I3P, or Dartmouth College.

1 Introduction

Outsourcing has been widely adopted in many industries. Within the IT function, the benefits of subcontracting specific technology services and entire business processes include cost reductions, improved utilization of core IS resources, and the acquisition of new technical skills and competencies (DiRomualdo and Gurbaxani 1998). Recent technology innovations allowing increased network bandwidth, processing virtualization, and inexpensive storage have pushed outsourcing to a new level by facilitating the migration of many internal IT applications to externally provided services. In this so called Software as a Service (SaaS) model, business applications are provided on demand as a service to customers. SaaS allows firms to reduce many fixed costs associated with the required internal IT infrastructure, application deployment, testing, maintenance, and patch management. It also lowers cost through competition. If a firm is not satisfied with a service provider, they can migrate to another provider without losing significant upfront investments (those investments would represent a sunk cost if the firm had entered into a long-term contract with an outsourcing vendor). Furthermore, enterprises using a service-oriented architecture (SOA) can segment processes and outsource them to different service providers. For example, within the financial services industry, many institutions rely heavily on both traditional outsourcing and SaaS, employing thousands of vendors that support their business processes.

While these different forms of outsourcing provide enterprise customers with both flexibility and cost benefits, the use of external service providers handling sensitive business data introduces new security risks (Macura and Johnson 2009). Many widely publicized security breaches have been the result of a partner failure. Sometimes these failures stem from neglect or under-investment in security. In other cases, the security challenges arise from the nature of the service provider's business model. Providers, who frequently enhance their service offering in response to evolving customer demand, introduce the possibility of new security bugs with every additional feature. Traditional methods in software assurance, with significant code testing, can be time consuming, slowing the vendor's ability to compete and tempting them to cut corners.

Of course a second worry is the firm's sensitive data that may be stored on a provider's machines and handled by employees of the service provider. That data represents a significant risk because the firm no longer has the ability to directly monitor and control its access. Even if the vendor's network is secure, the firm faces many web-based threats (hacking, malicious code etc.) when data is moving from the provider's facility over the Internet. Lastly, service providers often employ a model of multi-tenancy, where many enterprise customers share the same business application infrastructure with controlled access to their own data. The challenge for such a provider is segregating the customers' data. Inadequate data management may allow one firm's data to be exposed to another customer, which may be a competitor in the same industry.

For all of these reasons, firms must assess the information security level of their partners. Traditionally, customers perform such assessments through surveys, interviews, on-site visits, testing, and document review. Using that information the customers typically develop their own risk assessment (through identification of threats and vulnerabilities, control analysis, likelihood determination, risk determination etc.) (Stoneburner et al. 2002). This is time-consuming and costly for both vendors and customers. Since many firms (especially those in the financial industry) have hundreds of service providers, the time required to perform the risk assessment can make it impossible to assess every critical service provider.

Recently there have been several efforts to develop a common information security rating including the Business Information Technology Services (BITS) shared assessment, security vendor assessments (like Symantec's IT Risk Assessment) and most recently the collaboration between Goldman Sachs, Moody's, and Avior to create a Vendor Information Risk Rating (VIR). For example, in the Moody's rating, service providers who sign up are analyzed and rated in 11 "security fundamentals" categories, including access control, business continuity and data security (Scalet 2008). Two types of ratings are assigned to service providers - overall security quality ratings and inherent risk ratings (Macura and Johnson 2009). The information security rating helps to reduce time for enterprise customers to perform risk assessments by themselves (Kark 2008).

While it is tempting to directly equate information security rating with ratings of financial instruments, security ratings are quite different from credit ratings (which measure the default probability for a debt issuer). A good credit rating generally enables the debt issuer to raise money from the financial market at a lower cost (Kliger and Sarig 2000). However, a good security rating does not necessarily benefit a high-security service provider because the security rating may have subtle impacts on the competition among service providers, their incentives to improve security levels, and their prices charged to customers. In this paper, we focus on the following research questions:

- Does information security rating always benefit the high-security service provider (or hurt the low-security service provider), as the prior literature on finance predicts? If not, how does information security rating affect different service providers under different market conditions?
- Does information security rating always benefit the most demanding customers who desire highly secure business partners?
- Does information security rating increase social welfare?

In this paper, we develop an analytical model to examine the impact of information security ratings on service providers, customers, and social welfare. We do this by comparing two cases: (1) the case where an information security rating is provided, and (2) the case where customers perform risk assessments by themselves. It is commonly believed that information security rating benefits high-security service providers (and conversely hurts low-security providers). However, we find that, surprisingly, information security ratings can hurt or benefit both types of service providers, depending on the market conditions. Likewise, our analysis leads to another counterintuitive result: information security ratings can hurt demanding customers. Prior results in the licensing literature claimed that improved information always benefits the high-needs customers at the cost of less demanding customers (Shapiro 1986). We find cases where that is not true for information security.

We begin by examining the related literature, both in information security and finance. We discuss how information security ratings are different than ratings of financial instruments. In Section 2, we present our model, considering two types of service providers (low and high security) and two types of customers (those who place low and high value on security). We analyze the model for the case with professional information security ratings in Section 3, then the model for the case with customer assessments in Section **??**. We compare two cases in Section 5. Then we further compare the case with professional information security ratings and the case with no assessment in Section 6. Finally We conclude with recommendations for researchers and policy makers.

1.1 Literature Review

Rating the information security risk posed by business partners is a relatively new concept. Of course there is a substantial literature on financial risk rating, primarily focused on credit risk ratings and their impact on financial markets. For example, impact of credit risk rating on bond and stock prices (Hand et al. 1992, Kliger and Sarig 2000), capital structure decisions of managers

(Kisgen 2006), and credit default swap market (Norden and Weber 2004). In contrast with this stream of literature, we do not focus on the impact of information security rating on the financial market, but rather the impacts on service providers' profit, customers' net surplus, and social welfare. The finance literature generally assumes that the security risk is predetermined while the credit risk rating only plays a role of revealing information. In contrast, the security level of service provider in our paper is endogenously determined. The information security rating not only reveals information, but also influences the incentive of service providers' efforts on security.

A growing literature has examined the economics of information security from several different perspectives. Kannan and R. Telang (2005) compared a market-based mechanism and a Computer Emergency Response Team (CERT) mechanism for vulnerability disclosure. They found that the former mechanism almost always underperforms the latter one. Gal-Or and Ghose (2005) examined the value of information sharing about security breaches between competing firms. Arora, Telang and Xu (2008) further examined CERT's optimal timing of disclosing a vendor's software vulnerability. They found that the vendors may release patches later than is socially optimal when there is no forced disclosure. Thus, social planners could push vendors to release patches more quickly by threatening to disclose software vulnerabilities. Arora, Caulkins, and Telang (2006) used an analytical model to show that software vendors may have incentives to release buggier software early and patch it later. August and Tunca (2006) examined alternative policies to manage security in a network where vulnerabilities exhibit negative network externalities. They showed that the most effective policy is determined by considering the security risk and patching costs. August and Tunca (2008) further studied whether the users of unlicensed software should be provided the ability to apply security patches. They showed how the joint effects of software piracy and negative network security externalities affect the optimal policy choices. We examine the effects of vendor information security rating, which was not directly addressed in these papers.

2 The Model

We adopt a vertical differentiation framework (see, for example, Bhargava and Choudhary 2001, 2008) for customers who have different usage utilities for a business application service. We model two risk-neutral representative customers: (1) low-type customer, whose usage utility from the service is $V > 0$, and (2) high-type customer, whose usage utility from the service is θV with

$\theta > 1$.[2]

A service provider exerts effort e ($e \sim [0, 1]$) to increase the information security level of its service offering. We normalize the threat probability, the probability that the vendor is successfully breached, to $1 - e$. That is, when the service provider exert greater effort, it is less likely to be breached. The fixed cost of exerting effort e on security is assumed to be a convex function: ce^2, where $c > 0$ is the security cost parameter. Consistent with prior literature (August and Tunca 2006), when a breach occurs, the customer incurs a loss proportional to its usage utility. We use λV and $\lambda\theta V$ to denote the loss of the low-type customer and the high-type customer respectively, where $0 < \lambda < 1$.

ASSUMPTION 1: To focus on the interior solution, we assume that $V\theta\lambda/c < 1$, which ensures that the optimal efforts of both the low-security service provider (e_l^*) and high-security service provider (e_h^*) are less than 1.

The two service providers engage in a two-period competition. In Period 0, the service providers determine their security levels (that is, security efforts on information security). If a professional information security rating is provided in Period 1, the customers will know the security levels of both service providers. However, if a professional rating is not provided in Period 1, then the security levels of both service providers are unobservable to customers in Period 1. Service providers cannot hide their security levels forever. In time, the customers will eventually know the service providers' security levels in Period 2 via the customers' individual assessments. This means that the professional information security rating agencies are more efficient than individual customers (Kark 2008).

We allow service providers to adjust their prices at any time. That is, a service provider is able to charge a price in Period 2 different from that in Period 1.

For ease of exposition, we use e_l and e_h to denote lower and higher effort (or security level) respectively. p_l and p_h denote lower and higher price charged by service providers. π_l and π_h denote the total profit of lower and higher-security service providers in both periods. Next we analyze two cases: (1) when an information security rating is provided in Period 1, and (2) when customers perform risk assessments by themselves.

[2] A more general assumption is discussed in Subsection 8.12. It can be shown that the major results of this paper do not change.

V	low-type customer's usage utility from using the business application service
θV	high-type customer's usage utility from using the business application service, $\theta > 1$
λ	proportional loss of a customer's usage utility when a breach occurs
c	security cost parameter
e_h	security effort of high-security service provider
e_l	security effort of low-security service provider
p_h	price of high-security service provider
p_l	price of low-security service provider
p_i	introductory price of both service providers in Period 1 when information security ratings are not provided
π_h	profit of high-security service provider
π_l	profit of low-security service provider
$U\left(t, s, p\right)$	net surplus of a type-t customer who uses a business application service with a security level of s and a price of p
Case NR	the case where information security ratings are not provided in Period 1
Case R	the case where information security ratings are provided in Period 1
S1	the first scenario of Case NR, where only the high-type customer can afford p_i
S2	the second scenario of Case NR, where both types of customers can afford p_i
$\overline{p}_l^C$	average price of the low-security service provider in Case C $(C = NR, R)$
$\overline{p}_h^C$	average price of the high-security service provider in Case C $(C = NR, R)$

Table 1: Table of Notations

3 Competition with information security Ratings Provided

Information security ratings reveal the security levels of service providers to customers in Period 1. Hence, in this case customers know e_l and e_h in both periods. The competition in Period 1 is the same as that in Period 2. Hence, in Period 2, a service provider charges the same price as that charged in Period 1; a customer chooses the same service provider as that chosen in Period 1. Thus, we only need to focus on a single period.

We use $U(t, s, p)$ to denote the net surplus of a type-t customer who uses a business application service with a security level of s and a price of p, where $t = t_L$ (low-type customer) or t_H (high-type customer); $s = s_L$ (lower security level) or s_H (higher security level); $p = p_l$ or p_h. The expressions of $U(t, s)$ are as follows.

$$U(t_L, s_L, p_l) = e_l(V - p_l) + (1 - e_l)[(1 - \lambda)V - p_l]$$

$$U(t_L, s_H, p_h) = e_h(V - p_h) + (1 - e_h)[(1 - \lambda)V - p_h]$$

$$U(t_H, s_L, p_l) = e_l(\theta V - p_l) + (1 - e_l)[(1 - \lambda)\theta V - p_l]$$

$$U(t_H, s_H, p_h) = e_h(\theta V - p_h) + (1 - e_h)[(1 - \lambda)\theta V - p_h]$$

If both service providers stay in the market (i.e. high-security service provider sells to the high-type customer while low-security service provider sells to the low-type customer), then the low-security service provider can capture the low-type customer by charging a price p_l such that (IC1) $U(t_L, s_L, p_l) \geq U(t_L, s_H, p_h)$ (the low-type customer chooses the low-security service provider rather than the high-security service provider) and (IR1) $U(t_L, s_L, p_l) \geq 0$ (the low-type customer does not suffer a loss from using the service of the low-security service provider). Similarly, the high-security service provider should charge a price p_h such that (IC2) $U(t_H, s_H, p_h) \geq U(t_H, s_L, p_l)$ and (IR2) $U(t_H, s_H, p_h) \geq 0$. We claim that IR1 and IC2 are active (see Subsection 8.1 in Appendix for details). Given this fact, it is straightforward to verify that IR2 and IC1 can be neglected. Using

IR1 and IC2, we get

$$p_l = V\left(1-\lambda+\lambda e_l\right)$$
$$p_h = V\theta\lambda\left(e_h - e_l\right) + V\left(1-\lambda+\lambda e_l\right) \tag{1}$$

The low-security service provider obtains a revenue of p_l from the low-type customer in each period and thus, its total revenue is $2p_l$ in both periods. Likewise, the high-security service provider obtains a total revenue of $2p_h$ from the high-type customer in two periods. The total profits of the high-security service provider and low-security service provider in two periods can be written as follows.

$$\pi_l = 2p_l - ce_l^2$$
$$\pi_h = 2p_h - ce_h^2 \tag{2}$$

Inserting (1) in (2) and solving the first-order condition (F.O.C.) for optimal efforts, we obtain e_l^* and e_h^*. The second order conditions are satisfied because $d^2\pi_l/de_l^2 = d^2\pi_h/de_h^2 = -2c < 0$.

Proposition 1 *When an information security rating is provided to customers in the first period, then the optimal security efforts of high-security and low-security service providers are given by*

$$e_l^* = V\lambda/c,$$

$$e_h^* = V\theta\lambda/c.$$

The prices and profits of both service providers are given by $p_l^* = V\left(1-\lambda\right) + V^2\lambda^2/c$, $p_h^* = V\left(1-\lambda\right)+V^2\lambda^2\left[\theta\left(\theta-1\right)+1\right]/c$, $\pi_l^* = 2V\left(1-\lambda\right)+V^2\lambda^2/c$, $\pi_h^* = 2V\left(1-\lambda\right)+V^2\lambda^2\left[2-2\theta+\theta^2\right]/c$.

Next, we show that the high-security service provider does not have any incentive to compete the low-security service provider out of the market in equilibrium. If that happened, both types of customers would choose the high-security service provider even though the low-security service provider charges $p_l = 0$. That is, the high-security service provider must charge a price such that $U\left(t_L, s_H, p_h\right) \geq U\left(t_L, s_L, p_l\right)|_{p_l=0}$, $U\left(t_H, s_H, p_h\right) \geq U\left(t_H, s_L, p_l\right)|_{p_l=0}$. This leads to $p_h \leq \min\left[V\theta\lambda\left(e_h^* - e_l^*\right), V\lambda\left(e_h^* - e_l^*\right)\right] = V\lambda\left(e_h^* - e_l^*\right)$. Hence, if the high-security service provider charges $p_h = V\lambda\left(e_h^* - e_l^*\right)$, it will obtain a profit of $\pi_h = 4p_h - c\left(e_h^*\right)^2$ instead of $\pi_h^* = 2p_h^* - c\left(e_h^*\right)^2$. However, $\pi_h^* - \pi_h = \frac{2V}{c}\left[c\left(1-\lambda\right) + V\lambda^2\left(\theta^2 - 3\theta + 3\right)\right] > 0$ given $0 < \lambda < 1$ and $\theta > 1$. Therefore, two service providers share the market in equilibrium as shown in Proposition 1.

It can also be seen that the high-security service provider's optimal price, profit and security effort level are increasing functions of θ (the taste of high-type customer for the service). The intuition is that a higher θ increases the high-type customer's willingness-to-pay for the service in both scenarios: breached and unbreached. Hence, even though the high-security service provider keeps its security level the same as before, it still can increase its price and profit. But, a higher θ increases the marginal revenue $\left(d^2\left(2p_h\right)/\left(d\theta de_h\right) = 2V\lambda > 0\right)$ while does not affect the marginal cost $\left(d^2\left(-ce_h^2\right)/\left(d\theta de_h\right) = 0\right)$. Therefore, the high-security service provider still needs to increase its effort on security.

The low-security service provider's customer is not the high-type customer. It can be seen that the low-security service provider's optimal price, profit and effort on security level are not affected by θ.

Now, consider the effects of the customer's proportional loss from a breach (λ). Intuitively, both service providers should enhance their security levels when customers face a higher potential proportional loss. This can be seen from $de_l^*/d\lambda > 0$ and $de_h^*/d\lambda > 0$. However, the effects of a higher λ on optimal prices is not straightforward. We provide the following results.

Proposition 2 *If $\theta \geq 2$, then $dp_l^*/d\lambda < 0$ always holds. If $1 < \theta < 2$, then (1a) when $\theta V\lambda < c < 2V\lambda$, $dp_l^*/d\lambda > 0$; (1b) when $c \geq 2V\lambda$, $dp_l^*/d\lambda \leq 0$.*
(2a) When $\theta V\lambda < c < 2V\lambda\left(\theta^2 - \theta + 1\right)$, $dp_h^*/d\lambda > 0$;(2b) when $c \geq 2V\lambda\left(\theta^2 - \theta + 1\right)$, $dp_h^*/d\lambda \leq 0$.

When the cost of enhancing security (c) is sufficiently large, then a higher proportional loss from a breach (λ) results in a lower price $(p_l^*$ or $p_h^*)$. The reason is that a higher proportional loss from a breach (λ) reduces the customers' willingness-to-pay. Hence, the service providers need to reduce their prices if they cannot significantly enhance their security levels to increase the customers' willingness-to-pay. When the cost of security (c) is too large, then the incremental effort on security is so small that the service providers must reduce their prices. On the other hand, when the cost of security (c) is sufficiently small, then the service providers may be able to increase their prices because their security levels can be significantly enhanced.

4 Competition with Customer Assessments

In this section, we examine the case of competition where a professional information security rating is not provided in Period 1. We focus on the rational expectations equilibrium (Muth 1961), where customers form expectations on security levels of service providers, and the expectations are unbiased in equilibrium. That is, $E\left(e_l^*\right) = e_l^*$ and $E\left(e_h^*\right) = e_h^*$. We further assume that service providers can change their prices in no time. It follows that each service provider expects that lowering the price will immediately be met with the same move by the other firm. Thus, no service provider can expect to "steal" the other service provider's customers by simply cutting the price.

The security levels of service providers remain unknown to customers in Period 1. There are two possible equilibrium outcomes in Period 1: (a) a separating equilibrium where both service providers truly announce their types (high-security or low-security) and charge different prices on customers, and (b) a pooling equilibrium where the low-security service provider mimics the high-security service provider by charging the same price as that charged by the high-security service provider. It is easy to show that given e_l and e_h, the low-security service provider always has incentives to mimic the high-security one.

Thus, both service providers appear identical to customers, and they charge the same introductory price p_i; customers randomly choose a service provider in Period 1. We use $U\left(t,p\right)$ to denote the net surplus of a type-t customer who randomly chooses a service provider.

$$\begin{aligned} U\left(t_L,p_i\right) &= \tfrac{1}{2}E\left[U\left(t_L,s_L,p_i\right)\right] + \tfrac{1}{2}E\left[U\left(t_L,s_H,p_i\right)\right], \\ U\left(t_H,p_i\right) &= \tfrac{1}{2}E\left[U\left(t_H,s_L,p_i\right)\right] + \tfrac{1}{2}E\left[U\left(t_H,s_H,p_i\right)\right], \end{aligned} \tag{3}$$

where $E\left[U\left(t_L,s_L,p_i\right)\right] = E\left(e_l\right)\left(V-p_i\right)+\left(1-E\left(e_l\right)\right)\left[\left(1-\lambda\right)V-p_i\right]$, $E\left[U\left(t_L,s_H,p_i\right)\right] = E\left(e_h\right)\left(V-p_i\right)+\left(1-E\left(e_h\right)\right)\left[\left(1-\lambda\right)V-p_i\right]$, $E\left[U\left(t_H,s_L,p_i\right)\right] = E\left(e_l\right)\left(\theta V-p_i\right)+\left(1-E\left(e_l\right)\right)\left[\left(1-\lambda\right)\theta V-p_i\right]$, $E\left[U\left(t_H,s_H,p_i\right)\right] = E\left(e_h\right)\left(\theta V-p_i\right)+\left(1-E\left(e_h\right)\right)\left[\left(1-\lambda\right)\theta V-p_i\right]$.

There are two possible scenarios in equilibrium: (S1) only the high-type customer can afford the introductory price p_i in Period 1, and (S2) both types of customers can afford p_i in Period 1.

In the first scenario (S1), the expected demand of each service provider is $\frac{1}{2}$. The introductory price p_i is set to satisfy $U\left(t_H,p_i\right)=0$, or $p_i = V\theta\left(1-\lambda\right)+\frac{1}{2}\lambda\theta V\left[E\left(e_l\right)+E\left(e_h\right)\right]$. In Period 2, service providers charge different prices (p_h and p_l) because their security levels are revealed to customers via customers' risk assessments. Using a similar argument as that in Section 3, we get $p_l = V(1-\lambda+\lambda e_l)$ and $p_h = V\theta\lambda(e_h - e_l) + V(1-\lambda+\lambda e_l)$. The profits of low-security and high-security service providers can be expressed as: $\pi_l = \frac{1}{2}p_i + p_l - ce_l^2$ and $\pi_h = \frac{1}{2}p_i + p_h - ce_h^2$. We obtain the optimal efforts by solving the first order conditions of service providers.

In the second scenario (S2), the expected demand of each service provider is 1. The introductory price p_i satisfies $U(t_L, p_i) = 0$, or $p_i = V(1-\lambda) + \frac{1}{2}\lambda V[E(e_l) + E(e_h)]$. In Period 2, service providers charge p_l and p_h respectively when their efforts are revealed. The profits can be expressed as: $\pi_l = p_i + p_l - ce_l^2$ and $\pi_h = p_i + p_h - ce_h^2$. Again, we obtain the optimal efforts by solving the F.O.C. It can be shown that the second order conditions are satisfied.

Comparing the maximum profits obtained from S2 and from S1, we find that when $\theta > 2$, the maximum profits of both service providers in S1 are greater than those in S2. We summarize the results in the following proposition. The detailed proof is in the Appendix.

Proposition 3 *When $\theta > 2$, the optimal efforts of high-security and low-security service provider to enhance security level are given by*

$$e_l^* = V\lambda(4+\theta)/(8c),$$

$$e_h^* = 5V\theta\lambda/(8c).$$

The prices and profits of both service providers are given by $p_i^* = V\theta(1-\lambda) + V^2\lambda^2\theta(2+3\theta)/(8c)$, $p_l^* = V(1-\lambda) + V^2\lambda^2(4+\theta)/(8c)$, $p_h^* = V(1-\lambda) + V^2\lambda^2[4\theta^2 - 3\theta + 4]/(8c)$, $\pi_l^* = V(2+\theta)(1-\lambda)/2 + V^2\lambda^2\left[16 + 8\theta + 11\theta^2\right]/(64c)$, $\pi_h^* = V(2+\theta)(1-\lambda)/2 + V^2\lambda^2\left(19\theta^2 - 16\theta + 32\right)/(64c)$. *Only the high-type customer can afford p_i^* in Period 1.*

When $1 < \theta \leq 2$, the optimal efforts of high-security and low-security service provider to enhance security level are given by

$$e_l^* = 3V\lambda/(4c),$$

$$e_h^* = V\lambda(1+2\theta)/(4c).$$

Both service providers only sell to the high-type customer in Period 1. The prices and profits of both *service providers are given by* $p_i^* = \frac{V}{4c}\left[4c(1-\lambda) + V\lambda^2(2+\theta)\right]$, $p_l^* = V(1-\lambda) + 3V^2\lambda^2/(4c)$, $p_h^* = V(1-\lambda) + V^2\lambda^2\left(2\theta^2 - 2\theta + 3\right)/(4c)$, $\pi_l^* = 2V(1-\lambda) + V^2\lambda^2(11+4\theta)/(16c)$, $\pi_h^* = 2V(1-\lambda) + V^2\lambda^2\left(4\theta^2 - 8\theta + 19\right)/(16c)$. *Both types of customers can afford* p_i^* *in Period 1.*

In this section, the service providers appear identical to customers in Period 1. Thus, the service providers cannot segment the market by selling to different types of customers. Instead, the service providers have the same chance to sell to a specific type of customer. When the high-type customer has sufficiently high willingness-to-pay for the service (θ sufficiently large, $\theta > 2$), the target customer is high-type customer only. Otherwise, target customers are both types of customers.

5 Comparison: Professional Information Security Ratings versus Customer Assessments

We use Case R to denote the case where a professional information security rating is provided in Period 1, and Case NR to denote the case where a professional information security rating is not provided in Period 1 (that is, customers need to perform risk assessments by themselves).

Free-riding arises in Case NR because the low-security service provider may minic a high-security service provider, and then confuse customers. Intuitively, the free-riding problem should reduce the high-security service provider's incentive to invest in security. But, it is not obvious how the low-security service provider's security effort is affected. There are two conflicting effects. First, the low-security service provider appears identical to the high-security service provider in Period 1, so it could have incentives to enhance its security level to increase the willingness-to-pay of customers. Second, the low-security provider still needs to maintain an appropriate differentiation with the high-security provider in Period 2 to avoid intense price competition after security levels are known to customers. Since free-riding reduces the high-security provider's effort on security, the low-security provider could also reduce its effort to keep an appropriate differentiation with the high-security provider.

Proposition 4 *When a professional information security rating is not available, free-riding reduces the security effort of the high-security service provider. It also reduces the security effort of the low-security service provider when* $1 < \theta \leq 4$*, but increases its effort when* $\theta > 4$.

When $\theta > 2$, only the high-type customer can afford the introductory price (p_i^*) in Period 1 of Case NR (see Proposition 3). In Period 1 of Case NR, the low-security service provider sells to the high-type customer instead of the low-type customer (in Case R). When the high-type customer's taste is sufficiently large ($\theta > 4$), the low-security service provider will increase its effort on security because the gains from the high-type customer in Period 1 exceeds the loss from a narrower differentiation between the two service providers (which can cause intense price competition in Period 2).

Proposition 5 *The information security rating benefits both service providers when $\theta < \frac{5}{4}$. It hurts both service providers when $\theta > 2$ and $c > \frac{V\lambda^2[96+(45\theta-112)\theta]}{32(\theta-2)(1-\lambda)}$. It benefits the high-security service provider but hurts the low-security service provider in other regions.*

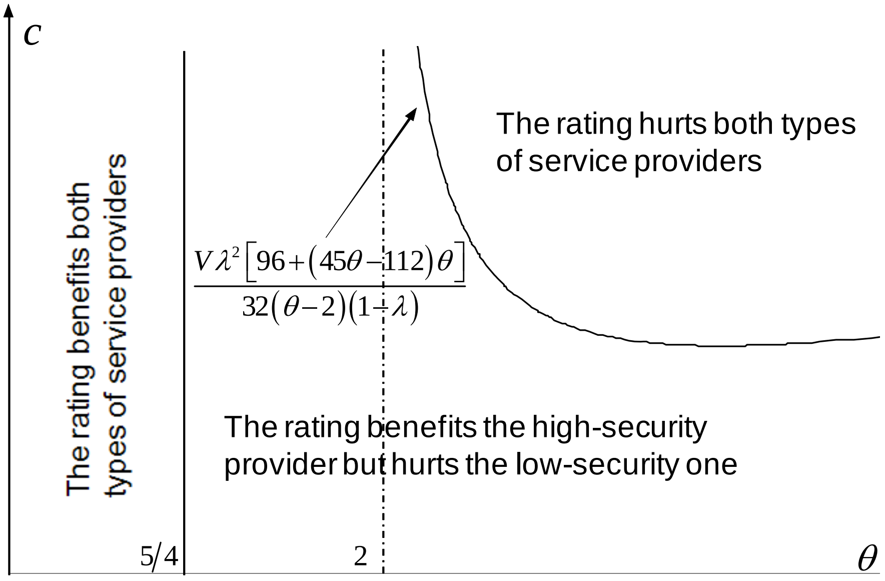

Figure 1: Impact of Rating on Service Providers' Profit ($V = 1$, $\lambda = 0.3$)

Figure 1 illustrates the result of proposition 5. It might seem intuitive that the information security rating always helps the high-security provider but hurts the low-security provider. Proposition 5 shows that it is *not always* the case. The reason is that information security rating generates two effects on the competition: (1) It eliminates the free riding problem. This effect helps the two service providers to differentiate themselves.[3] Thus, the information security rating can benefit

[3] In Case R, $e_h^* - e_l^* = \frac{V\lambda}{c}(\theta - 1)$. In Case NR, $e_h^* - e_l^* = \frac{V\lambda}{2c}(\theta - 1)$ for both S1 and S2. Clearly, $\frac{V\lambda}{c}(\theta - 1) > \frac{V\lambda}{2c}(\theta - 1)$, showing that the difference between e_h^* and e_l^* in Case R is larger than that in Case NR.

both service providers when both types of customers are not significantly differentiated ($\theta < \frac{5}{4}$). (2) It can intensify the competition in Period 1. In Case NR, when $\theta > 2$, the high-security provider can extract all the surplus from the high-type customer while the low-security provider can charge a high price by free-riding on the high-security provider. However, these benefits for both service providers are gone when the information security rating is provided. When it is hard to enhance the security (c is large), it will be useful for service providers to soften their competition. Thus, the information security rating (which can intensify the competition) may hurt both service providers.

Proposition 6 *The information security rating does not affect the low-type customer, whose net surplus is always zero. It benefits the high-type customer except when $\theta > 12$, $\frac{8\theta}{3(3\theta-4)} < \lambda < 1$, and $V\lambda\theta < c \leq \frac{V\lambda^2(\theta-12)}{8(1-\lambda)}$.*

This result is different from Shapiro (1986), which showed that improved information *always* helps the high-type customer. The reason is that Shapiro (1986) assumed that the market is fully competitive with no profit for the sellers while we do not make such an assumption. Footnote 10 of Shapiro (1986) suggested that modeling heterogeneous sellers would permit the analysis of issues not modeled in that paper. The sellers in our paper are heterogeneous.

Intuitively, information security rating helps the high-type customer to choose the high-security service provider, and thus benefits the high-type customer. Hence, it seems quite counterintuitive that the information security rating can hurt the high-type customer. The reasons for such counterintuitive result are as follows. Although information security rating encourages the high-security service provider to enhance its security, it can reduce the low-security provider's effort on its security (when $\theta > 4$, see Proposition 4). Then, the high-type customer's alternative choice (low-security service provider) in Period 2 is worse than when the rating is not provided in Period 1. This means that the high-security provider need not give the high-type customer a high net surplus to convince it not to choose the low-security provider. Therefore, the information security rating can hurt the high-type customer.

Proposition 5 and Proposition 6 have important managerial implications for the business model of the information security rating industry. For examples, the Moodys rating service charged service providers to conduct the assessment and also charged customers interested in the providers' ratings (the ratings were not publically available, but rather were provided for a fee). Our results suggest that it is not a good business model under certain conditions (for example, when both service providers are hurt by the information security rating). As shown above, information security ratings have a substantial effect on competition, the service providers, and customers. Information security rating agencies must understand these effects to assess the customers and service providers willingness to pay for the rating service.

Let $\overline{p}_l^{NR}$ be the average price of the low-security service provider in Case NR (that is, $(p_i^* + p_l^*)/2$ in Case NR), while $\overline{p}_l^R$ is for Case R (that is, p_l^* in Case R). Let $\overline{p}_h^{NR}$ and $\overline{p}_h^R$ be the average price of the high-security service provider in Case NR and Case R respectively.

Proposition 7 *If $\theta > 2$, then $\overline{p}_l^{NR} > \overline{p}_l^R$, otherwise $\overline{p}_l^{NR} \leq \overline{p}_l^R$. If $\theta > 2$ and $c > \frac{3V\lambda^2(3\theta^2-5\theta+4)}{8(\theta-1)(1-\lambda)}$, then $\overline{p}_h^{NR} > \overline{p}_h^R$, otherwise $\overline{p}_h^{NR} \leq \overline{p}_h^R$.*

From Proposition 3, we see that when $\theta > 2$, only the high-type customer can afford p_i^* in Period 1 of Case NR. Since the low-security service provider appears to be identical to the high-security service provider, it can charge a higher price than that in Case R (where it sells to the low-type customer, who has lower willingness-to-pay for the service than the high-type customer). This explains why $\overline{p}_l^{NR} > \overline{p}_l^R$ holds only when $\theta > 2$. Now, consider the average price of the high-security service provider. In Case NR, the free-riding problem always reduces the high-security provider's effort. It can reduce the willingness-to-pay of the high-type customer and thus the price charged by the high-security provider. On the other hand, the competition can be softened in Case NR because the high-security provider can now charge a high price such that the high-type customer's net surplus is 0. Whereas the high-security provider cannot do so in Case R because it needs to give the high-type customer positive net surplus to ensure that the customer would not choose the low-security service provider ($U(t_H, s_H, p_h) = U(t_H, s_L, p_l) > 0$). Thus, the effect of "softening competition" in Case NR tends to helps the high-security service provider to charge a higher average price than in Case R. When c is large ($c > \frac{3V\lambda^2(3\theta^2-5\theta+4)}{8(\theta-1)(1-\lambda)}$), the latter effect (softening competition) on average price is greater than the former effect (free riding problem).

Proposition 8 *Information security rating increases social welfare.*

Information security rating is a relatively new service compared to credit rating. In 1931, credit ratings were first endorsed by the US Office of the Comptroller of the Currency (OCC), which required banks to use current market prices for all bonds on their balance sheet rated below "investment grade". In 1936, the OCC went further and restricted banks from buying bonds below “investment grade”. In comparison, information security ratings are not officially endorsed by the US government. Proposition 8 suggests that social planners should encourage adoption of information security rating through public policy initiatives.

6 Robustness Check: Professional Information Security Ratings versus No Assessment

In Section 4, customers perform risk assessments by themselves. Although customers are not as efficient as professional information security rating agencies, they still know the security levels of service providers in Period 2. In this section, we assume that customers do not perform risk assessments at all. That is, even in Period 2, they are still not quite sure about service providers' security levels. Service providers announced their information breaches[4] at the end of Period 1. Then customers use such information to update their beliefs in Period 2.

Again, we focus on the rational expectations equilibrium (Muth 1961). As shown in Section 4, both service providers appear identical to customers because the low-security service provider would minic the high-security service provider. That is, customers believe that both service providers have a probability of $\frac{1}{2}$ to be a high-security service provider.

In Period 2, customers update their beliefs after observing incidents of information breach in Period 1. There are two possible scenarios: (1) one service provider suffers from an information breach while the other one does not, (2) both service providers suffer from information breaches or nobody suffers from any information breach (that is, both service providers still appear to be the same to customers).

We use B to represent “information breach”, NB to represent “no information breach”, H to represent “high-security service provider”, L to represent “low-security service provider”. It follows that HB means that “the high-security service provider suffers from an information breach”, LNB means that “the low-security service provider does not suffers from any information breach”, etc.

We proceed to caculate customers' updated beliefs in Period 2 in two possible scenarios. In the first scenario where only one service provider suffers from an information breach, customers' belief

[4] For example, Heartland Systems announced its information security breach shortly after the breach happened. See: http://seekingalpha.com/article/120694-heartland-systems-how-did-the-information-breach-happen

on the service provider affected by the information breach is updated as follows.

$$\begin{aligned}\Pr(L|B) &= \Pr(L)\Pr(LB, HNB)/[\Pr(L)\Pr(LB, HNB)+\Pr(H)\Pr(HB, LNB)] \\ &= \left[\tfrac{1}{2}(1-E(e_l))E(e_h)\right]/\left[\tfrac{1}{2}(1-E(e_l))E(e_h)+\tfrac{1}{2}(1-E(e_h))E(e_l)\right] \\ &= E(e_h)[1-E(e_l)]/[E(e_l)+E(e_h)-2E(e_h)E(e_l)] \\ &= e_h[1-e_l]/[e_l+e_h-2e_he_l].\end{aligned}$$

The last equation holds because we assume that customers form rational expectations on service providers' efforts on security. Using similar caculations, we obtain the following results.

$$\begin{aligned}\Pr(H|B) &= e_l[1-e_h]/[e_l+e_h-2e_he_l]. \\ \Pr(H|NB) &= e_h[1-e_l]/[e_l+e_h-2e_he_l]. \\ \Pr(L|NB) &= e_l[1-e_h]/[e_l+e_h-2e_he_l].\end{aligned}$$

The service provider who suffers from the information breach will charge a lower price in Period 2 while the one who does not suffer from any information breach will charge a higher price.

In the second scenario where both service providers suffer from information breaches or nobody suffers from any information breach, customers' beliefs on both service providers do not change. That is, both providers still have a probability of $\frac{1}{2}$ to be a high-security service provider. This result can be obtained by using a similar Bayesian belief updating as above. Since both service providers still appear to be the same to customers, they will continue to charge the same price to customers.

Proposition 9 *When customers do not perform any assessment, both service providers exert the same effort to enhance their security level. If $\theta > 2$, then $e_h^* = e_l^* = V\theta\lambda/(2c)$, $p_h^* = p_l^* = V\theta(1-\lambda)+V^2\theta^2\lambda^2/(2c)$, $\pi_h^* = \pi_l^* = V\theta(1-\lambda)+V^2\theta^2\lambda^2/(4c)$; if $\theta \leq 2$, then $e_h^* = e_l^* = V\lambda/(2c)$, $p_h^* = p_l^* = p_i = V(1-\lambda)+V^2\lambda^2/(2c)$, $\pi_h^* = \pi_l^* = 2V(1-\lambda)+3V^2\lambda^2/(4c)$.*

This suggests that customers' Bayesian belief updating does not provide enough incentives to service providers to develop a higher-security service than that of its competitor. This is because significant uncertainty still exists in Period 2. Even though a high-security service provider does not suffer from any information breach in Period 1, customers are still not quite sure that it is a high-security provider. Customers' willingness-to-pay for its service may increase (given that the low-security one incurs an information breach), but the incremental willingness-to-pay is small because customers still suspect that it is just a "lucky" low-security service provider in Period 1. Even worse, customers' willingness-to-pay for the high-security service in Period 2 can be lower than that in Period 1 when the high-security service provider is unlucky: its system suffers from an information breach in Period 1 while the low-security service provider does not.

In contrast, high-security service provider's security level is revealed in Period 1 when professional information security ratings are provided, or is revealed in Period 2 when customers perform their own risk assessments. It is straightforward to verify that both mechanisms motivate the high-security service provider to provide a better service than that when there is no information rating and customer risk assessment. Now, we can compare two cases: (1) the case where information security ratings are provided in Period 1, and (2) the case where no information security ratings and customer assessments are provided. By comparing two cases, we examine how information security ratings affect service provider profit and social welfare.

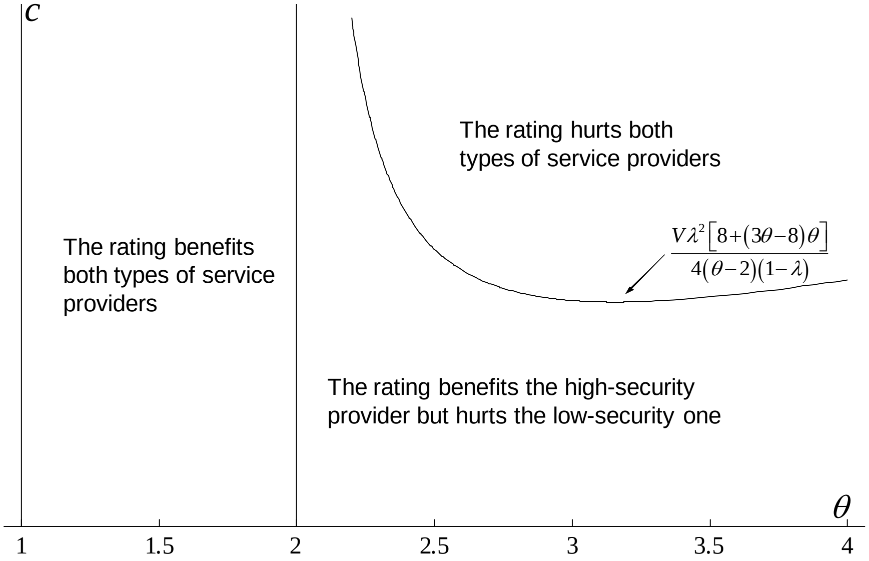

Figure 2: Impact of Rating on Service Providers' Profit ($V = 1$, $\lambda = 0.3$)

Proposition 10 *The information security rating benefits both service providers when $\theta < 2$. It hurts both service providers when $\theta > 2$ and $c > \frac{V\lambda^2[8+(3\theta-8)\theta]}{4(\theta-2)(1-\lambda)}$. It benefits the high-security service provider but hurts the low-security service provider in other regions. It increases the social welfare.*

Figure 2 shows the impact of information security ratings on service providers. The results of Proposition 10 are similar to those of Proposition 5 and Proposition 8, showing that the major results of Section 5 are robust.

7 Conclusion

There is growing interest in many industries for vendor information security rating services, which enable enterprise customers to obtain risk assessments of their service providers expeditiously. We investigate the impact of such information security rating services on customers, service providers and social welfare.

Intuitively, observers may conclude that information security ratings should benefit the high-security service providers and hurt the low-security ones. However, we find that this is not always the case - information security ratings can hurt both high-security and low-security service providers. This occurs when the absence of a security rating softens competition allowing the low-security service provider to appear identical to the high-security service provider. In that case, the low-security provider is able to charge a higher price than otherwise and the high-security service provider is able to avoid providing a positive net surplus to the high-type customer to guarantee that the customer does not choose the low-security provider. Therefore, it is possible that the information security rating can intensify competition and hurt both service providers. On the other hand, in some cases information security ratings can benefit both service providers. For example, in cases where the high-type customer is not significantly different from the low-type customer, it is useful for both service providers to differentiate their services though security to avoid head-to-head price competition. Since ratings clearly reveal the security of providers, such information helps service providers differentiate themselves and thus can benefit both.

Prior literature showed that improved information always benefits the high-type customer (Shapiro 1986). Our model shows that information security ratings can hurt the high-type customer. This is because our model captures competition between heterogeneous providers while Shapiro (1986) assumed homogeneous providers where profit is competed away. Hence, the improved information did not affect the competition in Shapiro's model. We consider a duopolist competition, where both service providers can earn a positive profit. We find that information security ratings have subtle effects on the competition. When the rating is provided, it may reduce the low-security service provider's incentives to invest in security. This reduces the quality of the alternative choice for the high-type customer. Thus, the high-security service provider will not need to provide a large net surplus to lure the high-type customer. This explains why the high-type customer can be hurt by an information security rating of providers.

Although the information security rating has subtle effects on service providers and customers respectively, it always increases the social welfare. The policy implication is that information security rating should be encouraged by social planners.

References

[1] Arora, A., R. Telang, and H. Xu. 2008. "Optimal Policy for Software Vulnerability Disclosure", *Management Science*, 54(4), 642-656.

[2] Arora, A., J. P. Caulkins, and R. Telang. "Sell First, Fix Later: Impact of Patching on Software Quality", *Management Science*, 52(3), 465-471.

[3] August, T., and T. I. Tunca. 2006. "Network Software Security and User Incentives", *Management Science*, 52(11), 1703-1720.

[4] August, T., and T. I. Tunca. 2008. "Let the Pirates Patch? An Economic Analysis of Software Security Patch Restrictions", *Information Systems Research*, 19(1), 48-70.

[5] Bhargava, H., and V. Choudhary. 2001. "Information Goods and Vertical Differentiation", *Journal of Management Information Systems*, 18(2), 89-106.

[6] Bhargava, H., and V. Choudhary. 2008. "Research Note: When is Versioning Optimal for Information Goods?" *Management Science*, (forthcoming).

[7] Calder, A., J. V. Bon, and V. Haren. 2006. "Information Security Based on ISO 27001/ISO 17799: A Management Guide", Van Haren Publishing, Zaltbommel, Netherlands.

[8] Dichev, I., J. Piotroski. 2001. “The Long-Run Stock Returns Following Bond Ratings Changes”, *The Journal of Finance*, 56(1), 173-203.

[9] DiRomualdo, A., and V. Gurbaxani. 1998. “Strategic Intent for IT Outsourcing”, *Sloan Management Review*, 39(4), 67-80.

[10] Gal-Or, E. and Ghose, A. (2005) “The Economic Incentives for Sharing Security Information”, *Information Systems Research*, (16)2, pp. 186-208.

[11] Hand, J., R. Holthausen, and R. Leftwich. 1992. “The Effect of Bond Rating Agency Announcements on Bond and Stock Prices”, *The Journal of Finance*, 47(2), 733-752.

[12] Kannan, K., and R. Telang. 2005. “Market for Software Vulnerabilities? Think Again”, *Management Science*, 51(5), 726-740.

[13] Kark, K. 2008. “Can Moody’s Solve Your Third Party Assessment Problem?” http://blogs.forrester.com/srm/2008/05/can-moodys-solv.html.

[14] Kisgen, D. 2006. “Credit Ratings and Capital Structure,” *The Journal of Finance*, 61(3), 1035-1072.

[15] Kliger, D., and O. Sarig. 2000. “The Information Value of Bond Ratings”, *The Journal of Finance*, 55(6), 2879-2902.

[16] Macura, I. and E. Johnson. 2009. “Information Risk and the Evolution of the Security Rating Industry,” *Working Paper*, Tuck School of Business at Dartmouth College.
http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/InfoRR7.pdf

[17] Muth, J. F. 1961. “Rational Expectations and the Theory of Price Movements”, *Econometrica*, 29(3), 315-335.

[18] Norden, L., and M. Weber. 2004. “Informational Efficiency of Credit Default Swap and Stock Markets: The Impact of Credit Rating Announcements”, *Journal of Banking & Finance*, 28(11), 2813–2843.

[19] Scalet, S. 2008. “Moody’s Wants to Rate Security, Not Just Securities”, *CIO Magazine*, February 26.

[20] Shapiro, C. 1986. “Investment, Moral Hazard, and Occupational Licensing”, *The Review of Economic Studies*, 53(5), 843-862.

[21] Stoneburner, G., A. Goguen, and A. Feringa. 2002. “Risk Management Guide for Information Technology Systems”, National Institute Standards and Technology (NIST) Special Publication 800-30.

8 Appendix

8.1 IR1 and IC2 are Active

Proof. We claim that IR1 is active (that is, $U(t_L, s_L, p_l) = 0$). If not, then both service providers will increase their prices until $U(t_L, s_L, p_l) = 0$ is satisfied. This is because (1) $p_h \leq V\theta\lambda(e_h - e_l) + p_l$ according to IC2; (2) it follows that IR2 is inactive: $U(t_H, s_H, p_h) = U(t_L, s_L, p_l) + V(\theta - 1)(1 - \lambda) + V\lambda(\theta e_h - e_l) + p_l - p_h \geq U(t_L, s_L, p_l) + V(\theta - 1)(1 - \lambda) + V\lambda(\theta e_h - e_l) + p_l - [V\theta\lambda(e_h - e_l) + p_l] = U(t_L, s_L, p_l) + V(\theta - 1)(1 - \lambda) > 0$. Thus, both service providers may increase their prices by the same amount without breaking any constraints listed above.

Further, IC2 is also active (that is, $U(t_H, s_H, p_h) = U(t_H, s_L, p_l)$). If not, then the high-security service provider can increase p_h until $U(t_H, s_H, p_h) = U(t_H, s_L, p_l)$ is satisfied (that is, $p_h = V\theta\lambda(e_h - e_l) + p_l$) without breaking the constraint IR2. This is because $U(t_H, s_H, p_h) = V(\theta - 1) \times (1 - \lambda + \lambda e_l) > 0$ when $p_h = V\theta\lambda(e_h - e_l) + p_l$ and $U(t_L, s_L, p_l) = 0$. Thus, both IR1 and IC2 are active. ■

8.2 Proof of Proposition 1

Proof. $d(\pi_l)/de_l = d\left(2p_l - ce_l^2\right)/de_l = d\left[2V(1 - \lambda + \lambda e_l) - ce_l^2\right]/de_l = 2V\lambda - 2ce_l$. Hence, $d(\pi_l)/de_l = 0$ leads to $e_l^* = V\lambda/c$. $d\pi_h/de_h = d\left(2p_h - ce_h^2\right)/de_h$
$= d\left[2V\theta\lambda(e_h - e_l) + 2V(1 - \lambda + \lambda e_l) - ce_h^2\right]/de_h = 2V\theta\lambda - 2ce_h$. Hence, $d\pi_h/de_h = 0$ leads to $e_h^* = V\theta\lambda/c$. Inserting e_l^* and e_h^* in (1) and (2) gives p_l^*, p_h^*, π_l^*, and π_h^*. ■

8.3 Proof of Proposition 2

Proof. $dp_l^*/d\lambda = \left(\frac{2V\lambda}{c} - 1\right)V$. According to Assumption 1, $V\theta\lambda/c < 1$, or $c > V\theta\lambda$. If $\theta \geq 2$, then $\frac{2V\lambda}{c} \leq \frac{\theta V\lambda}{c} < 1$, and thus $dp_l^*/d\lambda < 0$ always holds. If $1 < \theta < 2$, then when $\frac{2V\lambda}{c} - 1 \leq 0$, or $c \geq 2V\lambda > V\theta\lambda$, we have $dp_l^*/d\lambda \leq 0$; when $\frac{2V\lambda}{c} - 1 > 0$, or $c < 2V\lambda$, we have $dp_l^*/d\lambda > 0$.

$dp_h^*/d\lambda = V\left[\frac{2V\lambda}{c}\left(\theta^2 - \theta + 1\right) - 1\right]$. Solving $dp_h^*/d\lambda = 0$ for c yields $c = 2V\lambda\left(\theta^2 - \theta + 1\right)$. It easy to verify that $2V\lambda\left(\theta^2 - \theta + 1\right) > \theta V\lambda$. Hence, we get the results of the second part of Proposition 2. ■

8.4 Proof of Proposition 3

Proof. In the first scenario (S1), $p_i = V\theta\left(1-\lambda\right) + \frac{1}{2}\lambda\theta V\left[E\left(e_l\right) + E\left(e_h\right)\right]$, $p_l = V\left(1-\lambda+\lambda e_l\right)$, thus $\pi_l = \frac{1}{2}p_i + p_l - ce_l^2 = \frac{1}{2}\left[V\theta\left(1-\lambda\right) + \frac{1}{2}\lambda\theta V\left[E\left(e_l\right)+E\left(e_h\right)\right]\right] + V\left(1-\lambda+\lambda e_l\right) - ce_l^2$. Since customers form correct expectations on e_l and e_h, we have $E\left(e_l\right) = e_l$ in equilibrium. Inserting $E\left(e_l\right) = e_l$ in π_l and solving the F.O.C. for e_l^*, we may get $e_l^* = V\lambda\left(4+\theta\right)/\left(8c\right)$. Using a similar analysis, we may get $e_h^* = 5V\theta\lambda/\left(8c\right)$. Inserting e_l^* and e_h^* in p_i, p_h, p_l, π_l, and π_h, we may get p_i^*, p_h^*, p_l^*, π_l^*, and π_h^*. Using a similar argument, we may get results for the second scenario (S2).

The difference between π_h^* in S1 and S2 is $\left(\pi_h^*|\text{S1}\right) - \left(\pi_h^*|\text{S2}\right) = \frac{V}{64c}\left(\theta-2\right)\times$ $\left[32c\left(1-\lambda\right) + V\lambda^2\left(22+3\theta\right)\right]$. Clearly, it is greater than 0 when $\theta > 2$. Further, $\left(\pi_l^*|\text{S1}\right) - \left(\pi_l^*|\text{S2}\right) = \frac{V}{64c}\left(\theta-2\right)\times\left[32c\left(1-\lambda\right) + V\lambda^2\left(14+11\theta\right)\right] > 0$ when $\theta > 2$. ■

8.5 Proof of Proposition 4

Proof. We use the results of Proposition 1 and Proposition 3. $\left(e_h^*|\text{Case R}\right) - \left(e_h^*|\text{S1, Case NR}\right) = 3V\theta\lambda/\left(8c\right) > 0$, $\left(e_h^*|\text{Case R}\right) - \left(e_h^*|\text{S2, Case NR}\right) = V\lambda\left(2\theta-1\right)/\left(4c\right) > 0$. $\left(e_l^*|\text{Case R}\right) - \left(e_l^*|\text{S1, Case NR}\right) = V\lambda\left(4-\theta\right)/\left(8c\right) \geq 0$ when $\theta \leq 4$ but < 0 when $\theta > 4$, $\left(e_l^*|\text{Case R}\right) - \left(e_l^*|\text{S2, Case NR}\right) = V\lambda/\left(4c\right) > 0$. ■

8.6 Proof of Proposition 5

Proof. When $\theta > 2$, the equilibrium is S1 in Case NR (see proof of Proposition 3). $\left(\pi_h^*|\text{Case R}\right) - \left(\pi_h^*|\text{S1, Case NR}\right) = \frac{V}{64c}\left[V\lambda^2\left(45\theta^2 - 112\theta + 96\right) - 32c\left(\theta-2\right)\left(1-\lambda\right)\right]$ is greater than zero when $c > \frac{V\lambda^2\left[96+\left(45\theta-112\right)\theta\right]}{32\left(\theta-2\right)\left(1-\lambda\right)}$, and less than or equal to zero otherwise. $\left(\pi_l^*|\text{Case R}\right) - \left(\pi_l^*|\text{S1, Case NR}\right) = \frac{V}{64c}\left[-V\lambda^2\left(11\theta^2 + 8\theta - 48\right) - 32c\left(\theta-2\right)\left(1-\lambda\right)\right] < 0$. When $1 < \theta \leq 2$, the equilibrium is S2 in Case NR (see proof of Proposition 3).

$\left(\pi_h^*|\text{Case R}\right) - \left(\pi_h^*|\text{S2, Case NR}\right) = \frac{V^2\lambda^2}{16c}\left(12\theta^2 - 24\theta + 13\right) > 0$ in $\theta \in (1,2]$. $\left(\pi_l^*|\text{Case R}\right) - \left(\pi_l^*|\text{S2, Case NR}\right) = \frac{V^2\lambda^2}{16c}\left(5-4\theta\right) > 0$ in $\theta \in (1, \frac{5}{4})$ but ≤ 0 in $\theta \in [\frac{5}{4}, 2]$. ■

8.7 Proof of Proposition 6

Proof. Let ns_h^C be the net surplus of the high-type customer in Case C ($C = NR$, R). $ns_h^R = 2U\left(t_H, s_H, p_h\right) = \frac{2V}{c}\left(\theta-1\right)\left(c - c\lambda + V\lambda^2\right)$. When $1 < \theta \leq 2$, $ns_h^{NR} = U\left(t_H, p_i\right) + U\left(t_H, s_H, p_h\right) = \frac{V}{4c}\left(\theta-1\right)\left[8c\left(1-\lambda\right) + V\lambda^2\left(5+\theta\right)\right]$. $ns_h^R - ns_h^{NR} = \frac{V^2\lambda^2}{4c}\left(4\theta - \theta^2 - 3\right) > 0$. When $\theta > 2$, $ns_h^{NR} =$

$U(t_H, p_i) + U(t_H, s_H, p_h) = 0 + U(t_H, s_H, p_h) = \frac{V}{8c}(\theta - 1) \times \left[8c(1-\lambda) + V\lambda^2(4+\theta)\right]$. $ns_h^R - ns_h^{NR} = \frac{V}{8c}(\theta-1)\left[8c(1-\lambda) + V\lambda^2(12-\theta)\right] > 0$ when $c > \frac{V\lambda^2(\theta-12)}{8(1-\lambda)}$. According to Assumption 1, $c > V\lambda\theta$. Only when $\frac{V\lambda^2(\theta-12)}{8(1-\lambda)} > V\lambda\theta$, $V\lambda\theta < c \leq \frac{V\lambda^2(\theta-12)}{8(1-\lambda)}$ is possible. Solving the inequality $\frac{V\lambda^2(\theta-12)}{8(1-\lambda)} > V\lambda\theta$, we get $\theta > 12$ and $\frac{8\theta}{3(3\theta-4)} < \lambda < 1$. ■

8.8 Proof of Proposition 7

Proof. When $\theta > 2$, the equilibrium is S1 in Case NR (see proof of Proposition 3). $\left[\frac{1}{2}(p_l^* + p_i^*) \mid \text{S1, Case NR}\right] - [p_l^* | \text{ Case R}] = \frac{V}{16c}\left[8c(\theta-1)(1-\lambda) + 3V\lambda^2\left(\theta^2+\theta-4\right)\right] > 0$. $\left[\frac{1}{2}(p_h^* + p_i^*) \mid \text{S1, Case NR}\right] - [p_h^* | \text{ Case R}] = \frac{V}{16c}\left[8c(\theta-1)(1-\lambda) - 3V\lambda^2\left(3\theta^2 - 5\theta + 4\right)\right] = \Delta avgp_h$. Clearly, given θ, λ, and V, $\Delta avgp_h > 0$ when c is sufficiently large ($c > \frac{3V\lambda^2\left(3\theta^2-5\theta+4\right)}{8(\theta-1)(1-\lambda)}$).

When $1 < \theta \leq 2$, the equilibrium is S2 in Case NR (see proof of Proposition 3).
$\left[\frac{1}{2}(p_l^* + p_i^*) \mid \text{S2, Case NR}\right] - [p_l^* | \text{ Case R}] = \frac{V^2\lambda^2}{8c}(\theta - 3) < 0$. $\left[\frac{1}{2}(p_h^* + p_i^*) | \text{S2, Case NR}\right] - [p_h^* | \text{ Case R}]$ $= \frac{V^2\lambda^2}{8c}\left(-3 + 7\theta - 6\theta^2\right) < 0$. ■

8.9 Proof of Proposition 8

Proof. Let SW^C be the social welfare in Case C ($C = NR$, R). Note that the net surplus of the low-type customer is zero, we have $SW^R = ns_h^R + \pi_h^* + \pi_l^* = \frac{V}{c}\left[2c(\theta+1)(1-\lambda) + V\lambda^2\left(1+\theta^2\right)\right]$. When $\theta > 2$, $SW^{NR} = ns_h^{NR} + \pi_h^* + \pi_l^* = \frac{V}{32c}\left[32c(2\theta+1)(1-\lambda) + V\lambda^2\left(8 + 8\theta + 19\theta^2\right)\right]$; $SW^R - SW^{NR} = V(1-\lambda) + \frac{V^2\lambda^2}{32c}\left(13\theta^2 - 8\theta + 24\right) > 0$. When $1 < \theta \leq 2$, $SW^{NR} = \frac{V}{8c}[16c(\theta+1)(1-\lambda)$ $+V\lambda^2\left(5 + 6\theta + 4\theta^2\right)]$; $SW^R - SW^{NR} = \frac{V^2\lambda^2}{8c}\left(4\theta^2 - 6\theta + 3\right) > 0$ in $\theta \in (1, 2]$. ■

8.10 Proof of Proposition 9

Proof. Firstly we analyze the case where $e_h^* > e_l^*$.

(A) $e_h^* > e_l^* \geq 0$

In Period 1, both service providers appear identical to customers and then charge the same price p_i to customers. If only the high-type customer can afford the price in Period 1 (p_i), then we have $U(t_H, p_i) = 0$ (see Eq.3). That is,

$$pr_{mix}(\theta V - p_i) + (1 - pr_{mix})\left[(1-\lambda)\theta V - p_i\right] = 0,$$

where $pr_{mix} = \frac{1}{2}e_l + \frac{1}{2}e_h$. Solving this equation, we get

$$p_i = \frac{1}{2}V\theta \left[2\left(1-\lambda\right) + \lambda\left(e_h + e_l\right)\right]. \tag{4}$$

The expected demand of each service provider is $\frac{1}{2}$. Thus, the revenue of each service provider is

$$\pi_{S1} = \frac{1}{2}p_i = \frac{1}{4}V\theta \left[2\left(1-\lambda\right) + \lambda\left(e_h + e_l\right)\right]. \tag{5}$$

If both the high-type and the low-type customers can afford the price in Period 1 (p_i), then we have $U\left(t_L, p_i\right) = 0$

$$pr_{mix}\left(V - p_i\right) + \left(1 - pr_{mix}\right)\left[\left(1-\lambda\right)V - p_i\right] = 0.$$

Solving the above equation, we get

$$p_i = \frac{1}{2}V \left[2\left(1-\lambda\right) + \lambda\left(e_h + e_l\right)\right]. \tag{6}$$

The expected demand of each service provider is 1. Thus, the revenue of each service provider is

$$\pi_{S2} = 1 \cdot p_i = \frac{1}{2}V \left[2\left(1-\lambda\right) + \lambda\left(e_h + e_l\right)\right]. \tag{7}$$

Comparing π_{S1} and π_{S2}, we have $\pi_{S1} - \pi_{S2} = \frac{1}{4}V\left(\theta - 2\right)\ \left[2\left(1-\lambda\right) + \lambda\left(e_h + e_l\right)\right]$. Thus, when $\theta > 2$, both service providers charge a price such that only the high-type customer can afford it in Period 1. When $\theta \leq 2$, both service providers charge a price such that both types of customers can afford it in Period 1.

Now, consider Period 2. If both service providers suffer from information breaches or nobody suffers from any information breach, then customers' beliefs do not change and thus both service providers still charge the same price as that charged in Period 1. However, if only one service provider suffers from an information breach while the other one does not, then customers will believe that the service provider affected by the information breach has a higher probability to be a low-security service provider and thus can only charge a lower price than that charged by the other service provider. The lower price p_l satisfies

$$\Pr\left(NB|B\right)\left(V - p_l\right) + \left[1 - \Pr\left(NB|B\right)\right]\left[\left(1-\lambda\right)V - p_l\right] = 0, \tag{8}$$

where $\Pr(NB|B) = \Pr(L|B)\,e_l + \Pr(H|B)\,e_h$. Here $\Pr(NB|B)$ means "given that a service provider suffers from an information breach Period 1, the probability of that service provider not suffering from any information breach in Period 2"; $\Pr(L|B) = e_h[1-e_l]/[e_l+e_h-2e_he_l]$ means "given that a service provider suffers from an information breach in Period 1, the probability of that service provider being a low-security service provider"; $\Pr(H|B) = 1-\Pr(L|B)$. Solving Eq.(8) for p_l, we get

$$p_l = V(1-\lambda) + \frac{V\lambda e_h e_l (2-e_h-e_l)}{e_h+e_l-2e_he_l}.$$

The higher price p_h satisfies

$$\begin{aligned} &\Pr(NB|B)(V\theta - p_l) + [1-\Pr(NB|B)][(1-\lambda)V\theta - p_l] \\ &= \Pr(NB|NB)(V\theta - p_h) + [1-\Pr(NB|NB)][(1-\lambda)V\theta - p_h], \end{aligned} \tag{9}$$

where $\Pr(NB|NB) = \Pr(L|NB)\,e_l + \Pr(H|NB)\,e_h$, $\Pr(H|NB) = e_h[1-e_l]/[e_l+e_h-2e_he_l]$, $\Pr(L|NB) = e_l[1-e_h]/[e_l+e_h-2e_he_l]$. Solving Eq.(9) for p_h, we get

$$p_h = V(1-\lambda) + \frac{V\lambda\left[\theta(e_h-e_l)^2 + e_he_l(2-e_h-e_l)\right]}{e_h+e_l-2e_he_l}.$$

Thus, the Period 2 revenue of the service provider who has suffered from an information breach in Period 1 is

$$\pi_{L2} = p_l = V(1-\lambda) + \frac{V\lambda e_h e_l(2-e_h-e_l)}{e_h+e_l-2e_he_l}. \tag{10}$$

The Period 2 revenue of the service provider who does not suffer from any information breach is

$$\pi_{H2} = p_h = V(1-\lambda) + \frac{V\lambda\left[\theta(e_h-e_l)^2 + e_he_l(2-e_h-e_l)\right]}{e_h+e_l-2e_he_l}. \tag{11}$$

Now, we consider service providers' decisions of e_h and e_l at the begining of Period 1. We firstly consider the case where $\theta > 2$.

(A1) $\theta > 2$

The high-security service provider faces three possibilities as follows. (a) It does not suffer from any information breach while the low-security service provider suffers from an information breach in Period 1. This occurs at a probablity of $e_h (1 - e_l)$. The high-security service provider obtains a profit of $\pi_{S1} + \pi_{H2} - ce_h^2$ in this case. (b) It suffers from an information breach while the low-security service provider does not suffer from any information breach in Period 1. This occurs at a probablity of $e_l (1 - e_h)$. The high-security service provider obtains a profit of $\pi_{S1} + \pi_{L2} - ce_h^2$ in this case. (c) both service providers suffer from information breaches or nobody suffers from any information breach. This occurs at a probability of $e_h e_l + (1 - e_h)(1 - e_l)$. The high-security service provider obtains a profit of $\pi_{S1} + \pi_{S1} - ce_h^2$ in this case. Thus, the expected profit of the high-security service provider is

$$E(\pi_h) = e_h (1 - e_l)(\pi_{S1} + \pi_{H2}) + e_l (1 - e_h)(\pi_{S1} + \pi_{L2}) + [e_h e_l + (1 - e_h)(1 - e_l)](2\pi_{S1}) - ce_h^2, \tag{12}$$

where π_{S1}, π_{H2}, and π_{L2} are given by Eq.(5), Eq.(11), and Eq.(10) respectively. Similarly, we get the expected profit of the low-security service provider as follows.

$$E(\pi_l) = e_h (1 - e_l)(\pi_{S1} + \pi_{L2}) + e_l (1 - e_h)(\pi_{S1} + \pi_{H2}) + [e_h e_l + (1 - e_h)(1 - e_l)](2\pi_{S1}) - ce_l^2. \tag{13}$$

The first order conditions are given by $\partial E(\pi_h)/\partial e_h = 0$ and $\partial E(\pi_l)/\partial e_l = 0$. In the next paragraph, we show that $\partial E(\pi_l)/\partial e_l - \partial E(\pi_h)/\partial e_h > 0$ when $\partial E(\pi_l)/\partial e_l = 0$ and $e_h > e_l$. This means that $e_h^* > e_l^*$ is infeasible because $\partial E(\pi_h)/\partial e_h < 0$ and thus the high-security service provider has incentives to reduce its security level until $e_h = e_l^*$.

In this paragraph, we show that $\partial E(\pi_l)/\partial e_l - \partial E(\pi_h)/\partial e_h > 0$ when $\partial E(\pi_l)/\partial e_l = 0$ and $e_h > e_l$. Inserting Eq.(12) and Eq.(13) in $\partial E(\pi_h)/\partial e_h - \partial E(\pi_l)/\partial e_l$, we get $\partial E(\pi_l)/\partial e_l - \partial E(\pi_h)/\partial e_h = (e_h - e_l)[2c + V(\theta - 2) + \lambda V(4 - e_h - e_l)] + \frac{(e_h - e_l)V\theta\lambda}{2(e_h + e_l - 2e_h e_l)^2} t_0$, where $t_0 = -4e_h e_l (e_h^2 + 8e_h e_l + e_l^2) + 4e_h^2 e_l^2 (e_h + e_l) - (e_h + e_l)(e_h^2 - 30e_h e_l + e_l^2) - 4(e_h^2 + 4e_h e_l + e_l^2)$. According to Assumption 1, $c > V\theta\lambda$. Thus, $\partial E(\pi_l)/\partial e_l - \partial E(\pi_h)/\partial e_h > (e_h - e_l) \times [2V\theta\lambda + V(\theta - 2) + \lambda V(4 - e_h - e_l)] + \frac{(e_h - e_l)V\theta\lambda}{2(e_h + e_l - 2e_h e_l)^2} t_0 = \frac{(e_h - e_l)V}{2(e_h + e_l - 2e_h e_l)^2} t_1$, where $t_1 = 2[2\theta\lambda + \theta - 2 + \lambda(4 - e_h - e_l)](e_h + e_l - 2e_h e_l)^2 + \theta\lambda t_0$ is a linear function of λ. $t_1|_{\lambda=0} = 2(\theta - 2) \times (e_h + e_l - 2e_h e_l)^2 > 0$. $t_1|_{\lambda=1} = t_2\theta - 8e_h^2 e_l^2 (e_h + e_l) + 8e_h e_l \left[(e_h + e_l)^2 + 2e_h e_l\right] - 2(e_h + e_l) \times \left(e_h^2 + 10e_h e_l + e_l^2\right) + 4(e_h - e_l)^2$, where $t_2 = 4e_l e_h (1 - e_l)(1 - e_h)(e_h + e_l) + (e_h - e_l)^2 (2 - e_h - e_l) > 0$. Hence, $t_1|_{\lambda=1}$ is an increasing function of θ. Note that $\theta > 2$, we further caculate $t_1|_{\lambda=1,\theta=2} = 4\left[2e_h^2 + 2e_l^2 + 4e_h^2 e_l^2 - (e_h + e_l)^3\right] = (e_h + e_l)^2 (1 - e_h)(1 - e_l) + (e_h - e_l)^2 \left[1 - \frac{1}{4}(e_h + e_l)^2\right] + \frac{1}{4}(e_h + e_l)^4 >$

0. This shows that $t_1 > 0$ always holds. Thus, $\partial E(\pi_l)/\partial e_l - \partial E(\pi_h)/\partial e_h > \frac{(e_h-e_l)V}{2(e_h+e_l-2e_he_l)^2}t_1 > 0$.

(A2) $\theta \leq 2$

Using a similar proof of that for *(A1)* $\theta > 2$, we can also show that $e_h^* > e_l^*$ is infeasible.

(B) $e_h^* = e_l^* \geq 0$

When $e_h^* = e_l^*$ in equilibrium, customers will consider both service providers the same no matter who announces information breach in Period 2. Again, there are two subcases: $\theta > 2$ and $\theta \leq 2$.

(B1) $\theta > 2$

Let $e_h^* = e_l^* = e$. Both service providers' expected profit in two periods is $E(\pi) = 2\pi_{S1} - ce^2 = V\theta[(1-\lambda)+\lambda e] - ce^2$ (see Eq.(5)). Solving the F.O.C., we get we get $e_h^* = e_l^* = V\theta\lambda/(2c)$.

It can be verified that both service providers have no incentives to deviate. If a service provider deviates, say by reducing its security level from e to $e-\varepsilon$ $(\varepsilon > 0, \varepsilon \to 0)$, then its expected profit turns to be $E(\pi_{\varepsilon-}) = E(\pi_l)|_{e_h=e, e_l=e-\varepsilon}$ (see Eq.(13)). It can be shown that $E(\pi) - E(\pi_{\varepsilon-}) > 0$.[5] Similarly, it can also be shown that $E(\pi) - E(\pi_{\varepsilon+}) > 0$, where $E(\pi_{\varepsilon+}) = E(\pi_h)|_{e_l=e, e_h=e+\varepsilon}$.

Inserting $e_h^* = e_l^* = V\theta\lambda/(2c)$ in Eq.(4) and $E(\pi) = 2\pi_{S1} - ce^2$, we get $p_h^* = p_l^* = p_i = V\theta(1-\lambda) + V^2\theta^2\lambda^2/(2c)$, and $\pi_h^* = \pi_l^* = V\theta(1-\lambda) + V^2\theta^2\lambda^2/(4c)$.

(B2) $\theta \leq 2$

Both service providers' expected profit in two periods is $E(\pi) = 2\pi_{S2} - ce^2 = 2V[(1-\lambda)+\lambda e] - ce^2$ (see Eq.(7)). If a service provider deviates from e to $e-\varepsilon$ $(\varepsilon > 0, \varepsilon \to 0)$, then its profit will be

$$E(\pi_{\varepsilon-}) = e_h(1-e_l)(\pi_{S2}+\pi_{L2}) + e_l(1-e_h)(\pi_{S2}+\pi_{H2}) + [e_he_l + (1-e_h)(1-e_l)](2\pi_{S2}) - ce_l^2,$$

where $e_h = e$ and $e_l = e-\varepsilon$. It can be shown that $\lim_{\varepsilon\to 0}[E(\pi) - E(\pi_{\varepsilon-})]/\varepsilon = V\lambda - 2ce$. And $\lim_{\varepsilon\to 0}[E(\pi_{\varepsilon+}) - E(\pi)]/\varepsilon = V\lambda - 2ce$. Thus, $e_h^* = e_l^* = V\lambda/(2c)$. It follows $p_h^* = p_l^* = p_i = V(1-\lambda) + V^2\lambda^2/(2c)$, and $\pi_h^* = \pi_l^* = 2V(1-\lambda) + 3V^2\lambda^2/(4c)$. ■

8.11 Proof of Proposition 10

Proof. Consider the case where $1 < \theta \leq 2$. When information security ratings are provided in Period 1, then $(\pi_h^*|R) = 2V(1-\lambda) + V^2\lambda^2[2 - 2\theta + \theta^2]/c$; when there are no information security ratings and customer assessments, then $(\pi_h^*|NR) = 2V(1-\lambda) + 3V^2\lambda^2/(4c)$. $(\pi_h^*|R) - (\pi_h^*|NR) = V^2\lambda^2(4\theta^2 - 8\theta + 5)/(4c) > 0$ in $\theta \in (1,2]$. Further, $(\pi_l^*|R) - (\pi_l^*|NR) = V^2\lambda^2/(4c) > 0$. $SW^R -$

[5] $E(\pi)$ is not continous at $e_h^* = e_l^* = e$. There is a jump from $E(\pi_{\varepsilon-})$ to $E(\pi)$

$SW^{NR} = \frac{V}{2c}\left[V\theta\left(2\theta-1\right)\lambda^2 + 2c\left(1-\lambda\right)\left(\theta-1\right)\right] > 0.$

Consider the case where $\theta > 2$. $(\pi_l^*|R) - (\pi_l^*|NR) = -\frac{V}{4c}\left(\theta-2\right)\left[4c\left(1-\lambda\right) + V\lambda^2\left(2+\theta\right)\right] < 0$. $(\pi_h^*|R) - (\pi_h^*|NR) = \frac{V}{4c}\left[V\lambda^2\left(3\theta^2-8\theta+8\right) - 4c\left(\theta-2\right)\left(1-\lambda\right)\right]$. Clearly $(\pi_h^*|R) - (\pi_h^*|NR) < 0$ when $c > \frac{V\lambda^2\left(3\theta^2-8\theta+8\right)}{4(\theta-2)(1-\lambda)}$. Finally, $SW^R - SW^{NR} = \frac{V}{2c}\left[V\lambda^2\left(2+\theta^2\right) + 4c\left(1-\lambda\right)\right] > 0$. ■

8.12 Extension: Arbitrary Fraction of High-type and Low-type Customers

Proof. This paper assumes that there is a representative high-type customer and a representative low-type customer in the market. That is, the fraction of high-type are low-type customers in the market is 1 : 1. In this subsection, we allow the fraction of high-type and low-type customers to be $\alpha : 1$. Then, we will show that the major results of this paper do not change under the new assumption. To rule out trivial cases, we further assume that
Assumption E1: $\alpha > \max\left(1/\theta, 1/12\right)$.

Later it will be clear that this assumption ensures that the service provider who serves the high-type customer puts greater efforts on security than that who serves the low-type customer. And the profit of both service providers is greater than 0.

First, we consider the case where the information security rating is provided. Using a similar proof as that of Proposition 1, we have $U\left(t_H, s_H, p_h\right) = U\left(t_H, s_L, p_l\right)$ and $U\left(t_L, s_L, p_h\right) = 0$ in both periods. These eqalities lead to $p_h = V\theta\lambda\left(e_h - e_l\right) + V\left(1-\lambda+\lambda e_l\right)$ and $p_l = V\left(1-\lambda+\lambda e_l\right)$ in both periods. The high-security service provider's target is maximizing its profit $\pi_h = 2\alpha p_h - ce_h^2$. Solving the first order condition, we obtain $e_h^* = V\alpha\theta\lambda/c$. Using a similar argument, we obtain $e_l^* = V\lambda/c$. Clearly Assumption E1 ensures that $e_h^* > e_l^*$. Inserting e_h^* and e_l^* in p_h^*, p_l^*, π_l^* and π_h^*, we get $p_l^* = V\left(1-\lambda\right) + V^2\lambda^2/c$, $p_h^* = V\left(1-\lambda\right) + V^2\lambda^2\left[\theta\left(\alpha\theta-1\right)+1\right]/c$, $\pi_l^* = 2V\left(1-\lambda\right) + V^2\lambda^2/c$, $\pi_h^* = 2V\alpha\left(1-\lambda\right) + V^2\alpha\lambda^2\left[2-2\theta+\alpha\theta^2\right]/c$. It can be verified that when Assumption E1 is satisfied, then $\pi_h^* > 0$ and $\pi_l^* > 0$.

Second, we consider the case where the risk rating is not provided in Period 1. Again, there are two possible scenarioes: (S1) only the high-type customer can afford the introductory price p_i in Period 1, and (S2) both types of customers can afford p_i in Period 1.

Consider scenario S1, we have $e_h^* = V\lambda\left(1+\alpha+4\alpha\theta\right)/\left(8c\right)$, $e_l^* = V\lambda\left(5+\alpha\right)/\left(8c\right)$, $p_i^* = V\left(1-\lambda\right) + V^2\lambda^2\left[3+\alpha+2\alpha\theta\right]/\left(8c\right)$, $p_l^* = V\left(1-\lambda\right) + V^2\lambda^2\left(5+\alpha\right)/\left(8c\right)$, $p_h^* = V\left(1-\lambda\right) + V^2\lambda^2[5+\alpha]/\left(8c\right) + V^2\lambda^2\theta\left(\alpha\theta-1\right)/\left(2c\right)$, $\pi_h^* = V\left(1+3\alpha\right)\left(1-\lambda\right)/2 + V^2\lambda^2\left[11+\alpha(54-32\theta)+\alpha^2(11+16\theta^2)\right]/\left(64c\right)$, and $\pi_l^* = V\left(3+\alpha\right)\left(1-\lambda\right)/2 + V^2\lambda^2\left[27+\alpha^2\left(3+8\theta\right)+\alpha\left(14+8\theta\right)\right]/\left(64c\right)$.

Consider scenario S2, we have $e_h^* = 5V\alpha\theta\lambda/\left(8c\right)$, $e_l^* = V\lambda\left(4+\alpha\theta\right)/\left(8c\right)$, $p_i^* = V\theta\left(1-\lambda\right) + V^2\lambda^2\theta\left[2+3\alpha\theta\right]/\left(8c\right)$, $p_l^* = V\left(1-\lambda\right)+V^2\lambda^2\left(4+\alpha\theta\right)/\left(8c\right)$, $p_h^* = V\left(1-\lambda\right)+V^2\lambda^2[4\alpha\theta^2+\theta\left(\alpha-4\right)+4]/\left(8c\right)$, $\pi_h^* = V\alpha\left(2+\theta\right)\left(1-\lambda\right)/2+V^2\lambda^2 a\left[32+8\theta\left(\alpha-3\right)+19\alpha\theta^2\right]/\left(64c\right)$, and $\pi_l^* = V\left(2+\alpha\theta\right)\left(1-\lambda\right)/2+V^2\lambda^2\left[16+8\alpha\theta+11\alpha^2\theta^2\right]/\left(64c\right)$.

It can be verified that when $1 < \theta \leq \frac{1+\alpha}{\alpha}$, then $(e_h^*|\text{S1}) \leq (e_h^*|\text{S2})$ and $(e_l^*|\text{S1}) \leq (e_l^*|\text{S2})$; when $\theta > \frac{1+\alpha}{\alpha}$, then $(e_h^*|\text{S1}) > (e_h^*|\text{S2})$ and $(e_l^*|\text{S1}) > (e_l^*|\text{S2})$. That is, $(e_h^*|\text{Case NR}) = (e_h^*|\text{S2})$ and $(e_l^*|\text{Case NR}) = (e_l^*|\text{S2})$ when $1 < \theta \leq \frac{1+\alpha}{\alpha}$; $(e_h^*|\text{Case NR}) = (e_h^*|\text{S1})$ and $(e_l^*|\text{Case NR}) = (e_l^*|\text{S1})$ when $\theta > \frac{1+\alpha}{\alpha}$.

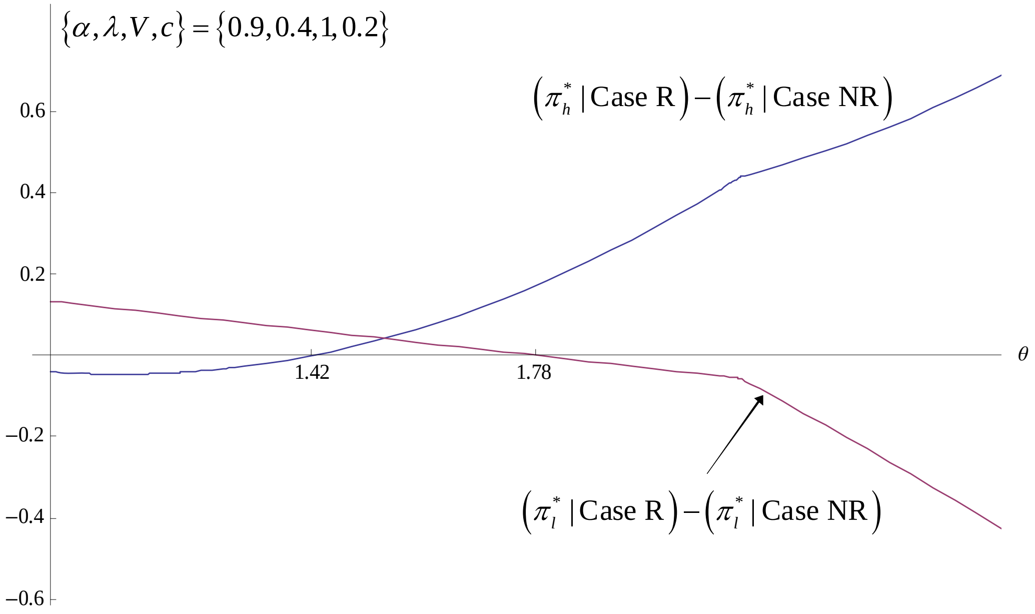

Figure 3: Impact of Rating on Service Providers' Profit

Figure 3 shows that when $\{\alpha, \lambda, V, c\} = \{0.9, 0.4, 1, 0.2\}$, then information security rating (1) hurts the high-security service provider while benefits the low-security service provider when $\theta < 1.42$, (2) benefits both types of service providers when $1.42 \leq \theta \leq 1.78$, and (3) benefits the high-security service provider while hurts the low-security service provider when $\theta > 1.78$.

Figure 4 shows that when $\{\alpha, \lambda, V, c\} = \{0.9, 0.4, 1, 1.2\}$, then information security rating (1) hurts the high-security service provider while benefits the low-security service provider when $\theta < 1.75$, (2) benefits both types of service providers when $1.75 \leq \theta \leq 2.15$, (3) benefits the high-security service provider while hurts the low-security service provider when $2.15 \leq \theta \leq 2.48$, and (4) hurts

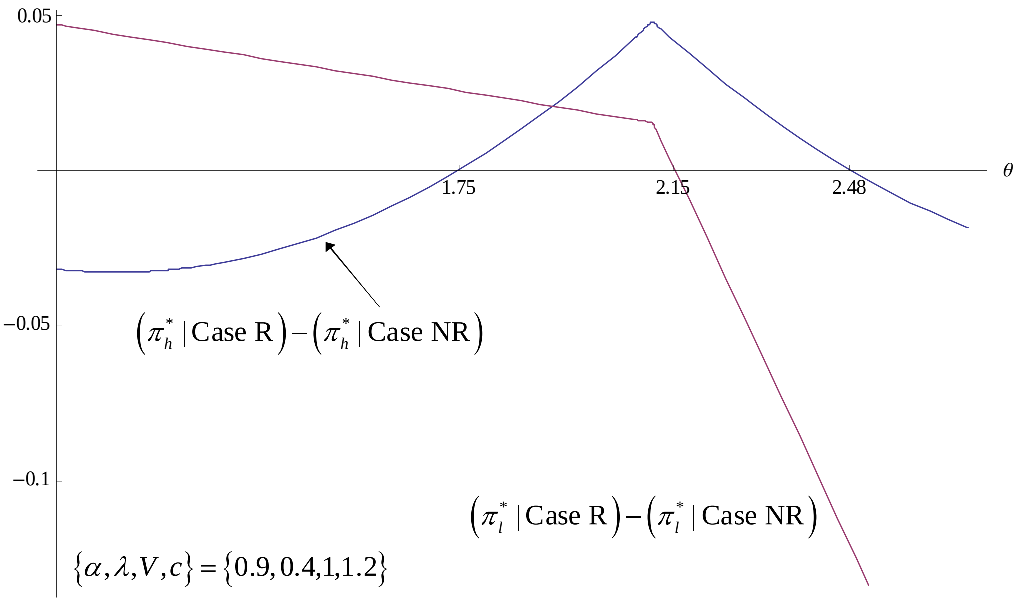

Figure 4: Impact Rating on Service Providers' Profit

both types of service providers when $\theta > 2.48$.

Therefore, we find cases where information security rating can (1) benefit both service providers, (2) benefit the high-security service provider while hurt the low-security service provider and (3) hurt both service providers. This shows that the major results of Proposition 5 do not change.

Interestingly, we find a new case - information security rating can benefit the low-security service provider while hurt the high-security service provider. This is because the market size of high-type customers is smaller than that of low-type customers in our numerical examples ($\alpha = 0.9 < 1$). If information security rating is not provided, the high-security service provider and the low-security service provider have the same expected demand, which is $(1 + 0.9)/2 = 0.95$. However, if information security rating is provided, the demand for the high-security service provider turns to be 0.9, which is smaller than 0.95. Thus, information security rating could hurt the high-security service provider by reducing the demand for its service.

It can be verified that when the market size of high-type customers is larger than that of low-type customers ($\alpha \geq 1$), then information security rating will not hurt the high-security service provider while benefit the low-security service provider. ■